At a Glance ▪ ▪ ▪

2 Community Services: Integrated Case Management System

Summary

The Department of Community Services and the Department of Internal Services do not have all the necessary controls in place to protect the privacy, integrity and availability of the data in the Integrated Case Management (ICM) system. Given that the system was implemented in 2007, we assessed the system against the processes and controls that would be expected around a mature IT environment. The following table shows the results of our assessment of the ICM system's controls.

Sections	Confidentiality	Integrity	Availability
Information Technology Security	●	○	○
IT Service Operations	○	○	●
Data Integrity	--	○	--
IT Governance	○	○	○

○ Improvements are required.
● Significant improvements are required.
-- Controls assessed in this section are not meant to address confidentiality or availability.

We noted that Community Services has made positive steps through initiatives in the areas of training, IT control assessments, IT technical forums and project management. However, we identified significant weaknesses in the IT security of systems. We also identified processes that need to be redesigned or enhanced, including those of IT risk management. These deficiencies put the confidentiality, integrity and availability of information within the ICM system at risk.

Confidentiality: Security weaknesses in the configuration of the system allowed us to gain unauthorized access to sensitive personal information maintained in ICM, including detailed case notes, names of children taken into care, and financial information. Access to this personal information is limited to users within the government network. Some of these weaknesses were subsequently addressed by Community Services after we communicated them.

Integrity: There are weaknesses in how ICM accepts and stores data, as well as in the processes around managing changes, user access and incidents. Incomplete and inaccurate information can negatively impact the decisions of those providing services.

Availability: There are deficiencies in monitoring system resources and availability; planning to restore ICM in the event of an outage; and central oversight of business continuity plans. The risk associated with these deficiencies is high because of the intermittent system outages ICM has been experiencing. Timely access to the client and case information within ICM is required for employees providing services to Nova Scotians.

2 Community Services: Integrated Case Management System

Background

2.1 The Department of Community Services (the Department) contributes to the health and well-being of Nova Scotians through the delivery of social programs. According to the Department's 2014 public statement of mandate, it provides services to approximately 200,000 Nova Scotians each year. This represents 1 in 5 Nova Scotians.

2.2 The cost to provide these services according to the Department's 2014-15 budgeted expenditures is approximately $904 million, with the majority of funding across four key divisions.

Divisions	Expenditure
Employment support and income assistance	$383 million
Family and children's services	$143 million
Services for persons with disabilities	$299 million
Housing services	$36 million
Other division expenditures	$43 million
Total	$904 million

2.3 The Integrated Case Management (ICM) system was developed and implemented in 2007 and is therefore expected to be a mature system. It is intended to help support the integral social service programs administered by the key divisions in the Department. ICM is a web-based application, only accessible by employees on the government network.

2.4 The application stores information that helps employees to track, manage and make decisions on the services they provide to their clients. These decisions include the following.

- Are the basic needs of the client being met?
- What assistance is the client eligible for?
- What assistance has the client received in the past?
- Is intervention and protection needed?

2.5 Given the nature of the services being provided, the information that is collected and stored in ICM can be highly sensitive and linked to specific individuals. This includes financial records, contact information, and records of services obtained from the Department. While the Department owns the

ICM application and is responsible for the data stored in it, the infrastructure that supports the application is managed by Information, Communication and Technology Services (ICTS), a branch of the Department of Internal Services. This branch was previously known as the Chief Information Office. That Office was created in April 2009.

2.6 The Information, Communication and Technology Services branch's mandate is to plan, organize and direct the efficient and effective use of information technology (IT) across government. It is responsible for the Provincial Government's IT infrastructure. This includes the government network, telecommunications and the Provincial data centre. ICTS provides and manages the servers and databases which support and run the Department of Community Services' Integrated Case Management system.

Audit Objectives and Scope

2.7 In summer 2014, we completed an audit of the Department of Community Service's Integrated Case Management system. The overall goal of the audit was to assess whether the Department has necessary controls to protect the confidentiality and integrity of the data in ICM, and to ensure its availability when providing services to clients.

2.8 Audit criteria for this engagement were based on the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT 4.1). COBIT is a widely-accepted, international source of best practices for the governance, control, management and audit of IT operations. The audit objectives and criteria were discussed with, and accepted as appropriate by, Department of Community Services' senior management.

2.9 Audit fieldwork was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards of CPA Canada. It was performed during the period from March to July 2014. Technical aspects of systems were assessed at various points in time from April to July of 2014 and system transactions were analyzed for the period of April 1, 2012 to February 28, 2014.

Significant Audit Observations

IT Security

Conclusions and summary of observations

We identified significant weaknesses in IT security. We were able to gain unauthorized access to confidential information contained in ICM. Information accessed included personal information such as detailed client case notes, details of client visits and financial information. We were also able to gain unauthorized access to information on four servers which we used to gain full control over two of those servers, and access to a database. Some of these weaknesses were subsequently addressed by the Department after we communicated them.

Servers are not fully secured against unauthorized access from within Government

2.10 *Background* – Information technology such as applications, databases and operating systems have settings (e.g., password length, logging of key system events, account lockout limits) that can be configured to dictate how users interact with them. Improper application of these settings can create security weaknesses, giving individuals the opportunity to gain unauthorized access to view, modify or delete information.

2.11 *Unauthorized access to reports* – ICM has reporting capabilities that are used to generate reports for staff and management to use in support of their job responsibilities. These reports may include information such as detailed history of case notes for a particular client, children taken into care, client contact information, client financial details, and a list of all ICM users and permissions.

2.12 We found significant security weaknesses that allowed us to view ICM reports and see sensitive information. Anyone within the government network could potentially view this information. When we informed Department management, they partially addressed the weaknesses to prevent anyone outside Community Services from accessing the sensitive information. Department management told us that they were not aware of any security breaches.

Operating system and database controls are not sufficient

2.13 *Operating system controls* – We assessed the security of the operating systems for the eight servers that support ICM. It is necessary to provide system administrators with accounts that allow them to manage and maintain the operating systems of the ICM servers (server accounts). These accounts are different from those used by Community Services staff to access ICM when providing services to clients. Specific roles assigned to the server accounts include:

- running the ICM application and its database;
- running tools to store and manage programming code for ICM;
- generating reports for ICM users; and
- executing scheduled programs to send and receive data.

2.14 We found deficiencies related to the server accounts which are detailed below.

2.15 *Unauthorized access to files* – We were able to gain unauthorized, read-only access to files and folders on four of the eight servers reviewed. Information viewed in some of these files contained user names and passwords which gave us the ability to have full control over two servers. Full control over these servers would allow a user to give access to other users, run programs, modify data, or shut down the system entirely. The user names and passwords we found also allowed us to gain access to a test database for ICM, which was populated with real client data as recent as 2012. ICM data can include case notes made by case workers, financial information and contact information of clients.

2.16 Prior to our audit, users connected to the government network (e.g. in all government departments) would have been able to access these confidential files. When we notified the Department, management addressed the weaknesses that were putting the security of the system at risk.

2.17 *Operating system versions* – Three of the eight servers used to support the ICM system are using versions which will no longer be supported by the vendor, and will no longer receive security and other updates, as of 2015. Without these updates, the servers could have weaknesses that would allow unauthorized individuals to gain access to the server or cause system outages.

2.18 *Passwords* – As noted above, server accounts are used for administration purposes or to assist in running ICM programs. The accounts are installed by the vendor of the operating system or created by the Province. To manage these accounts, each server has unique settings (e.g. passwords, account lockouts, and auditing) to prevent and detect unauthorized access to the server through these accounts.

2.19 We found the settings for account passwords were not consistently applied across all eight servers. Two of those servers' settings did not provide adequate security and did not match the password standards required by the Information, Communication and Technology Services branch. None of the eight servers have enabled account lockout functionality to restrict the number of unsuccessful logins a local user can have; therefore, attempts to log in can continue until unauthorized access is gained.

2.20 *User accounts* – We found unnecessary accounts on four of the eight servers we reviewed. This creates avoidable exposure to unauthorized system access.

2.21 *Database controls* – The detailed information about ICM clients is stored in its databases. The databases need to be protected to prevent someone from bypassing the ICM application controls in place and gaining direct access to data files. We noted weaknesses relating to the security of the databases. This includes lack of logging for key system events, such as unsuccessful login attempts, and weak database account and password settings.

▶ Information transferred internally is not encrypted

2.22 *Electronic data transfers* – We assessed the security of data transferred between ICM and other servers, databases and external entities. We noted information transmitted outside of the Province's network is encrypted. However, data transferred between databases or to users within the network is not always encrypted, thus increasing the risk of unauthorized capture and viewing of confidential data.

Recommendation 2.1
The Department of Community Services and the Department of Internal Services should address security weaknesses identified in ICM databases and servers.

Department of Community Services Response: The Department agrees with this recommendation. The Department, upon being informed of the identified weaknesses, immediately addressed significant findings. The Department will develop a work plan in collaboration with Information, Communications, and Technology Services (ICTS) to review existing technical settings and make appropriate changes.

Department of Internal Services Response: Information, Communication and Technology Services Branch, agrees with this recommendation. An implementation plan and timeline has been developed to address this recommendation.

IT Service Operations

Conclusions and summary of observations

There are weaknesses in the operational processes which manage ICM that put the confidentiality, integrity and availability of information at risk. During our testing, we noted that the processes to manage changes to programming code are ineffective. We also observed that the process to manage user access requires improvement in order to ensure all users have appropriate access to ICM. Further, additional oversight is required to manage incidents. We noted processes for identification and remediation of problems are informal. Also, there are deficiencies in monitoring system availability and more oversight is needed to ensure the Department's business continuity plans are documented, updated and tested. The Department's processes to manage projects related to ICM are good.

Additional access management controls are required

2.23 *Background* – User access to information systems needs to be carefully managed to ensure that information is only available to those who need to see it. When a user's responsibilities change, their access should change accordingly. Without strong controls over granting, modifying and removal of access to the ICM application, there is a risk that users could have access to information that is not required as part of their job responsibilities. This increases the risk of unauthorized disclosure, modification or deletion of data.

2.24 *User account management* – An employee requires both a government network account and an ICM account before being able to access the ICM application. ICTS is responsible for managing network accounts for all of government while the Department manages ICM accounts and grants permissions.

2.25 We tested various components of access management for ICM and found the following deficiencies.

- Access Management – There are processes in place to manage employee access to ICM. However, of a sample of 50 access requests for new users, we found one was granted a higher level of access than what was required for their job duties, and three did not have evidence of appropriate approvals for the access they received.
- Review of Existing Accounts – There is no formal process to review current users' level of access to information. We noted that three of 40 accounts tested had inappropriate access for their current job roles and responsibilities, therefore providing them with access to confidential information not required for their job.

- Dormant Accounts – We identified 59 accounts that were no longer required. Management subsequently disabled these accounts upon our notification.

Recommendation 2.2
The Department of Community Services should ensure only authorized users have access to only the information necessary to fulfill their job requirements and only for the period of time required.

Department of Community Services Response: The Department agrees with this recommendation. Periodic reviews of ICM security to ensure staff continues to have appropriate security levels are currently conducted. The current procedures will be reviewed and enhanced monitoring implemented.

Processes do not ensure timely problem resolution

2.26 *Background* – IT-related incidents are disruptions to users' ability to productively use information technology. Incidents need to be identified, documented and addressed to ensure staff can continue to perform their work and information remains secure. Recurring IT incidents can also add more strain on IT resources and require an effective problem management process to identify and address the root causes of those incidents.

2.27 *Incident management* – Incidents applicable to ICM that are identified by staff are communicated to the Department's IT Services group. IT Services utilizes a web application to record incident tickets, track, and monitor the resolution of those incidents. We noted that the Department does not review the status of the tickets that are on hold or in process to determine if they still need to be addressed or can be closed. Our review of ICM tickets identified several instances of open and pending tickets that were created in 2010, 2011 and 2012 which increases the risk of persistent issues within ICM.

2.28 *Problem management* – Management relies on staff awareness of recurring incidents to indicate there may be a larger problem. While the production support team holds bi-weekly meetings to discuss any recurring issues staff are aware of, they do not retain meeting notes. In addition, the software utilized to record and manage incidents is not used to analyze tickets to look for recurring issues or trends that may indicate a larger problem. Performing a proactive review of incident tickets could assist the Department in identifying recurring problems sooner and improving the overall quality and availability of the system.

Recommendation 2.3
The Department of Community Services should regularly analyze results of its reported incidents and take action to address weaknesses on a timely basis.

Department of Community Services Response: The Department agrees with the recommendation. A new Incident Management process is being developed and adopted which will ensure tickets are appropriately addressed and closed.

2.29 *Background* – Changes to information technology can result in the introduction of security vulnerabilities and programming errors if they are poorly managed. Therefore, changes should be approved, documented, tested, and approved prior to implementation. Larger changes require proper project management practices. Weaknesses in the processes to manage projects and ongoing changes to a system can result in weaknesses in the system such as programming bugs or security holes.

Project management practices are strong

2.30 *Project management* – Large changes undertaken by the Department are documented and managed through the use of strong project management practices which help to protect the confidentiality, integrity and availability of ICM. Such changes are major business improvement initiatives and include implementing ICM in other Departmental program areas. We reviewed the Department's documentation and process followed for one of four significant projects listed in the draft IT strategic plan and noted:

- a strong governance structure;
- an effective approach for the size and scope of the project;
- evidence of stakeholder commitment;
- maintenance of a detailed project plan throughout,
- identification and management of project risks;
- management of resources; and
- measurement of the performance of the project.

Change management practices have weaknesses

2.31 *Change management* – Changes to ICM can be minor, for example, new reports or adding options to dropdown menus. Changes can also be made to programming code. The Department has a process to make changes to ICM which includes using software to manage ICM programming code, track changes, and restrict who can make those changes. However, the process and associated approvals relating to these programming changes are not documented in a consistent manner and, in some cases, not documented at all. A lack of documented approvals and testing was found in five recent changes that we examined, indicating that changes may have been made without going through the proper approval and testing processes. Changes that are not controlled can increase risks to the system, such as system failures or lost client data.

Recommendation 2.4
The Department of Community Services should ensure documentation to support the management of changes to ICM is maintained, including its purpose, testing results and applicable approvals.

Department of Community Services Response: The Department agrees with this recommendation. The current Change Management process is being revised and will be adopted to ensure consistency and supporting documentation is maintained.

▶ Continued availability of ICM is at risk

2.32 *Background* – Employees should be able to access ICM in support of their job responsibilities at all times. Ensuring systems are available requires monitoring the hardware resources of servers, including how much memory and processing power is being utilized. In the event users experience an ICM system outage, management should have a plan to restore ICM and maintain the Department's services.

2.33 *Resource performance management* – Users have been experiencing ICM system outages. Community Services has hired consultants to assess the application, database and web server, however, the source of the issue has not been identified. The Department is still working on fixing the issue.

2.34 *Continuous monitoring* – The Department of Internal Services' Information, Communication and Technology Services branch (ICTS) uses a program to monitor the status of servers. Should a server fail or go offline, an alert can be sent to ICTS staff so the problem can be fixed. However, three of the eight ICM servers we reviewed did not have the program installed; therefore, ICTS staff would not be notified in a timely manner if those servers went down. Instead, the users would be the first to become aware of server issues through a system outage. On the five servers with the monitoring program installed, only the basic features have been enabled. Additional preventative settings could be enabled to send out alerts and warning prior to a server going down. However, Department management was unaware of further monitoring capabilities and the need to specifically request these services from ICTS.

Recommendation 2.5
The Department of Community Services and the Department of Internal Services should monitor the performance and capacity of the ICM systems on an ongoing basis and address any issues.

Department of Community Services Response: The Department agrees with this recommendation. The Department has already made several changes to improve the performance of ICM and will continue to improve system performance and work with Information, Communications, and Technology Services (ICTS) to put adequate monitoring tools in place.

Department of Internal Services Response: Information, Communication and Technology Services Branch, agrees with this recommendation and will work with the Department of Community Services to develop and implement a process to monitor the performance and capacity of the ICM systems on an ongoing basis and address any issues. An implementation plan will be developed with the Department of Community Services.

2.35 *Continuity planning* – Employees in each of the Department's four regions are assigned responsibility for business continuity planning to ensure that critical services provided by the Department can be maintained or resumed quickly in the event of an interruption. This would include natural disasters or a mass illness that reduce staffing levels. Without proper continuity planning, essential services to Nova Scotians could be disrupted in the event government offices or ICM are unavailable.

2.36 The Department of Community Services, in an oversight capacity, has not ensured that all locations have appropriate and current plans. The Department is working with ICTS to test a new, government-wide business continuity plan initiative that will assess requirements and develop standards to ensure all departments have effective plans. This includes prioritization and timelines for the restoration of key department-specific computer programs. Training is expected to be provided to government business continuity plan coordinators, culminating in a government-wide testing exercise in December 2014.

Recommendation 2.6
The Department of Community Services should ensure that business continuity plans are in place and contain information such as prioritization and timelines for restoration of key Department computer programs.

Department of Community Services Response: The Department agrees with this recommendation. The Department will complete its work with Information, Communications, and Technology Services (ICTS) on the business continuity plan initiative and will work to ensure all regional locations have current and appropriate business continuity plans that include information pertaining to the restoration of key computer programs.

2.37 *Disaster recovery* – As part of an audit reported in November 2011, our Office made a recommendation to ICTS to develop a disaster recovery plan for the

Provincial data centre. While a plan has been developed, it does not list the key departmental computer programs that need to be restored, or the priority and timeframes in which they should be restored. This information will be available from the business continuity plans prepared by the departments and should be incorporated into the Provincial disaster recovery plan.

Recommendation 2.7
The Department of Internal Services and the Department of Community Services should work together to incorporate the Department of Community Services' business continuity plan into the Province's disaster recovery plan.

Department of Community Services Response: The Department agrees with this recommendation. The Department will work with the Department of Internal Services to incorporate the Department's business continuity plan into the province's disaster recovery plan.

Department of Internal Services Response: Information, Communication and Technology Services Branch agrees with this recommendation and will work with the Department of Community Services to incorporate Department of Community Services' business continuity plan into the province's disaster recovery plan. An implementation plan and timeline is in place; significant progress has been made in identifying critical business functions and analysis of ICT requirements at the Department of Community Services.

Data Integrity

Conclusions and summary of observations

Weaknesses exist which pose a risk to the integrity of ICM information. We performed an analysis of the data stored in ICM and found potential areas of concern. We identified trends in data that showed payments without case numbers, duplicate clients and duplicate trustees in the system, and bank accounts which receive funds for multiple clients. These weaknesses create the potential for overpayments, payments to the wrong individuals, and decisions based on incomplete information.

2.38 *Background* – Data integrity is a term that encompasses essential characteristics that need to be in place in order for a system to adequately support operations. Those characteristics include data completeness, consistency, timeliness, and validity. Data integrity enables system users to make decisions based on reliable information and to appropriately identify and monitor operations.

Additional monitoring controls are required around ICM data

2.39 *Payments to clients* – We analyzed payments made between April 1, 2012 to February 28, 2014. In order for the Department to adequately monitor total payments made to, or on behalf of its clients, a case identification number should be assigned to all payments. We identified 0.04% , or 1,250, of approximately 3.1 million transactions that were not associated with case identification numbers and therefore could not be traced back to clients. We understand that the ability to enter payments without a case identification number is a necessity to provide immediate services to some clients but the lack of association with a case increases the risk for fraud and error.

Recommendation 2.8

The Department of Community Services should closely control and monitor the risks related to payments made without a case identification number.

Department of Community Services Response: The Department agrees with this recommendation. The ability to make low dollar value payments without a case identification number is necessary to provide immediate services to some clients, particularly Child Welfare cases. Payments without a case identification number accounted for 0.04% of payments made through ICM during the audit period. The Department will investigate the feasibility of using SAP, rather than ICM, for these types of payments to increase control.

2.40 *Bank account activity* – We performed an analysis to identify trends and anomalies related to client bank accounts to which payments are made. Although situations in which the same account is used for multiple individuals within the same family are expected, we found instances of the same bank account used for multiple individuals who were not family. For example, individual bank accounts were associated with as high as 205 and 435 different clients.

2.41 After researching the accounts noted above, it was found that the accounts were related to organizations providing services on behalf of clients (trustees). However, ICM does not have controls in place to monitor or verify that bank accounts are assigned to the appropriate individuals. If bank account assignments are not monitored, there is a risk that funds are deposited in accounts that do not belong to the client.

Recommendation 2.9

The Department of Community Services should enhance controls over bank account assignments to clients.

Department of Community Services Response: The Department agrees with this recommendation. The Department has established an internal working group to create an action plan to address this recommendation and other internal control improvements. Existing controls over bank accounts include the use of a direct deposit form, signed by the client, and supported by a voided cheque or bank stamp. The form has recently been reviewed and improvements have been made. Existing policies also require strict segregation of duties among Department staff when bank accounts are entered into ICM. These controls will be reinforced with Department staff.

Reliability of data is at risk due to weaknesses

2.42 *Duplicate client records* – We conducted an analysis to identify multiple occurrences of the same first name, last name, gender and birthdate within ICM. We found instances in which the same client had been entered four or more times. This limits the system's ability to identify all cases linked to a given client. One case number may not provide the whole picture of a client's interactions with the Department and decisions may be made using inaccurate or incomplete information.

2.43 The issue of duplicate client records was a known issue that the Department was in the process of correcting. The Department had corrected approximately 5,000 records already flagged as duplicates. However, even after the duplicate records are corrected, the potential for creating new duplicate records will still exist as the system does not prevent such situations. Management indicated that users need the flexibility to enter clients with limited amounts of information in order to provide essential services on a timely basis. Therefore, duplicate clients will continue to exist in ICM. Duplicate records make it difficult to obtain the entire case history for a given client and this increases the opportunity for fraud and error.

2.44 *Duplicate trustee records* – Some of the Department's clients require assistance to handle their payments. In these situations, specific individuals and organizations are designated as trustees and receive funds on behalf of the client. Trustees can assist multiple clients at the same time, but we found the Department re-enters trustee information for each client. We analyzed Department data and found that, in some instances, the same trustee was created more than 100 times. This results in an integrity issue because a client is associated with a trustee, but ICM does not link a given trustee to all the clients they represent. This raises concern about the ability to monitor the total activity of trustees and other organizations acting on behalf of various clients, and increases the opportunity for fraud and error.

Recommendation 2.10

The Department of Community Services should reduce duplicate clients and trustees within ICM.

Department of Community Services Response: The Department agrees with this recommendation. The Department will continue its ongoing efforts to reduce duplicate client records through staff training and monitoring. The use of a single bank account by multiple clients has increased in recent years due to use of large trustees such as shelters. The Department plans to prepare monthly reports showing all bank accounts assigned to more than one client, and to assign specific responsibility for monitoring these reports. In addition, the Department will examine the issue of how to specifically identify trustees and related clients in ICM.

IT Governance

Conclusions and summary of observations

Governance and oversight of information technology controls and processes are weak in some areas of the Department of Community Services. The Department has not implemented an IT risk management framework to assess, and potentially reduce, the impact of IT risks on the organization. Also, IT application controls have not been tested to ensure they are working as designed; and therefore, confidentiality, integrity and availability of data is at risk. We noted that while the Department aligns itself with the goals, policies and standards of the Provincial government and the Information, Communication and Technology Services branch, the Department's IT strategic plan is draft with outstanding sections to be completed. In addition, as noted throughout this chapter, there are many weaknesses which need oversight to address.

There is no IT risk management framework in place

2.45 *Background* – An IT risk management framework with continuous monitoring of controls and processes is required to protect the confidentiality, integrity and availability of information. Without identifying and assessing IT risks, the organization cannot be sure that it has the required safeguards in place to protect its assets. Without proper monitoring of these safeguards or controls, the organization cannot ensure existing safeguards are working effectively. These processes would oversee all IT controls and would assist in reducing the deficiencies identified in this chapter.

2.46 *IT risk management framework* – The Department does not have a complete IT risk management framework to identify, document and manage IT risks, including security threats and system outages. The Department relied on ICTS for risk management, but ICTS is still developing its IT risk management services and does not yet have the tools and policies needed for government-wide implementation. Risks which have not yet been identified, analyzed, and mitigated can result in vulnerabilities which could impact the confidentiality, integrity and availability of information.

2.47 The Department completed a self-assessment of its IT controls protecting the ICM application, using a comprehensive assessment template provided by ICTS. The assessment is a positive first step in identifying the existence of IT controls and any gaps in the controls. However, the Department did not test existing IT controls to assess if they were working as intended. Without assurance that controls are working as planned, there could be vulnerabilities which negatively impact the confidentiality, integrity and availability of information.

Recommendation 2.11
The Department of Community Services should ensure it has a control framework for IT which includes risk management and a plan to assess the ongoing effectiveness of controls.

Department of Community Services Response: The Department agrees with this recommendation. The Department will complete its IT risk management framework and will perform testing of existing IT controls to ensure their effectiveness.

▶ The IT strategic plan has not been finalized

2.48 *IT governance* – As outlined in Community Services' draft IT strategic plan, the Information and Technology Services group supports the Department's technology needs and aligns itself with the goals, policies and standards of the provincial government and ICTS. However, the current plan is still draft, with outstanding sections to be completed. Without a finalized strategic plan, there is a risk that the direction and prioritization of IT initiatives may not fully address the needs of the business. The Department's draft IT strategic plan identified the need for a decision-making group to determine the prioritization of initiatives outlined in the plan.

2.49 *Service-level agreements* – Daily support of the ICM system is a shared responsibility between ICTS and Community Services. ICTS hosts and monitors the ICM servers, while the Department is responsible for approving system access, and determining application and system monitoring requirements. The Department and ICTS do not have an operating agreement to outline the types of services provided and associated service-level expectations. Areas which should be covered in this agreement include:

- service desk responsibilities;
- ICM hosting requirements and performance targets;
- backup and recovery; and
- disaster recovery procedures and prioritization.

2.50 Without a service-level agreement, Community Services cannot ensure that ICTS has agreed to the requested services (e.g. application hosting, system monitoring, and disaster preparedness) to be performed to ensure the security of ICM and to prevent system outages.

Recommendation 2.12
The Department of Community Services should finalize an approved IT strategic plan that includes the role and responsibilities of the Information, Communication and Technology Services branch and the Department.

Department of Community Services Response: The Department agrees with this recommendation. The Department will finalize the IT strategic plan and will include roles and responsibilities of Information, Communciations, and Technology Services (ICTS) and the Department.

▶ IT training and IT security awareness training are being developed

2.51 *IT service training* – The Department has moved forward on initiatives to improve the services and processes of its IT Services group. This includes training and certifying staff on the Information Technology Infrastructure Library (ITIL) – a set of widely-used practices for IT service management that focuses on aligning IT services with the needs of business. In addition, the Department has implemented an IT technical forum to provide a venue for staff to discuss various IT issues, and identify and investigate problems or service enhancements.

2.52 *IT security awareness* – The Department has not provided security awareness training to its staff since 2011 and training is not routinely provided to new staff. Department management told us that they are creating a new training plan for information security awareness and is revamping its new staff orientation program. Employees can be targeted by malicious individuals in an attempt to get them to unknowingly disclose information or open vulnerabilities in computer systems that could be exploited. Employees need to be trained and made aware of the signs they are being targeted and how to respond appropriately. The Department is aware of the lack of IT security awareness training and told us it will be provided.