Department Audits

4 INFORMATION TECHNOLOGY AND FINANCIAL CONTROLS

BACKGROUND

4.1 Information technology impacts virtually every program and service administered by the Department of Community Services. Information technology is used to administer financial assistance and regulatory programs, pay suppliers, record operating transactions, as well as many other activities. The Department's widespread reliance on information technology has made control over information technology and related financial processes critical to efficient and effective departmental operations.

4.2 Community Services provides financial assistance to eligible persons under a number of programs, including the Employment Support and Income Assistance (ESIA) program. Under this program, income assistance payments are made by cheque or direct deposit. Direct deposit payments are made once a month by way of electronic funds transfers (EFT). The Department's Finance and Administration section is responsible for financial controls over ESIA program payments, supplier payments, and transaction recording as well as other financial controls.

4.3 The Department's Information Technology Services (ITS) section is responsible for managing the Department's information technology resources. The section's role is to maintain, improve and develop information technologies and services within the Department. Its key activities include acquiring information technology, setting access controls, supporting hardware and software, planning and training. The section is divided into three branches: technology infrastructure, production support and business solutions. ITS also provides services to the Department of Service Nova Scotia and Municipal Relations, the Children's Aid Societies, as well as to the regional housing authorities.

4.4 Community Services has invested approximately $8.4 million in information technology hardware and software since 1999 and is in the process of implementing a significant new system referred to as the integrated case management system. The budgeted cost of this new system is $11.4 million, of which $5.7 million has been incurred as at March 31, 2006.

4.5 At March 31, 2006, there were 41 ITS staff supporting 3,076 computer users located in offices throughout the Province. Community Services, the Children's Aid Societies, and the regional housing authorities account for 2,226 of these users.

4.6 The Department of Community Services incurred $341.6 million of expense under the Employment Support and Income Assistance program, $7.8 million for ITS operating expenses and $3.9 million for hardware and software purchases during the year ended March 31, 2006. Hardware and software purchases include costs of $2.7 million related to the integrated case management system.

RESULTS IN BRIEF

4.7 The following are our principal observations from this assignment.

- Certain controls over the Department's general computer environment and electronic funds transfers for income assistance were adequate. However, we also identified significant control weaknesses which overshadow and erode the controls which we assessed as adequate. Accordingly, we concluded control in these areas is generally inadequate.

- A number of the control weaknesses identified in this chapter pose a significant risk of financial loss or other negative consequences, either through fraudulent actions or error. We concluded there are inadequate compensating controls to address these significant weaknesses.

- We identified inadequate monitoring of shared passwords and inappropriate computer access. Also, access rights of staff members who leave the Department were not canceled on a timely basis.

- There are no computerized dollar limits on electronic funds transfer transactions and no computerized edit checks on data sent to the bank for processing payments. Bank reconciliations are not being properly completed, and review and approval processes are not documented.

- Information technology purchases are being properly approved, accurately recorded and are in accordance with Provincial procurement and accounting policies.

ASSIGNMENT SCOPE

4.8 In January 2006 we completed a review of the general computer environment controls and an audit of controls over electronic funds transfers and information technology purchases at the Department of Community Services. This work represents the second phase of an assignment commenced in 2005. Phase one examined operations of the Department relating to income assistance and employment support, and child care centre licensing. Observations from phase one were reported in Chapter 6 of the December 2005 Report of the Auditor General.

4.9 The scope of our review of general computer environment controls was limited to those for which the Department of Community Services has responsibility. The Department's information systems are integrated with other systems of the government of Nova Scotia, and certain information processing for Departmental programs is performed by entities external to the Department and government. We did not review any systems or controls operating outside the Department. Further, our review of the Department's information systems environment was restricted to staff interviews, observation of systems, review of documents and testing of access rights. We did not perform detailed testing of all systems to determine if controls described to us operated effectively throughout the period of our review. Accordingly, we offer a moderate level of assurance in our assessment of general computer environment controls. Audit level assurance is provided for our conclusions on controls over electronic funds transfers and information technology purchases.

4.10 The assignment was conducted in accordance with Section 8 of the Auditor General Act and assurance standards established by the Canadian Institute of Chartered Accountants, and accordingly included such tests and procedures as we considered necessary in the circumstances.

4.11 The objectives of this assignment were to:

- review general computer environment controls, including those relating to risk management, information technology planning, operations, security, change management, and end-user computing, as well as disaster recovery and business continuity planning;

- assess the adequacy of controls used to ensure electronic funds transfers for the Employment Support and Income Assistance program are complete, accurate, properly approved and for authorized purposes; and

- assess whether information technology purchases are properly approved, accurately recorded and in compliance with Provincial procurement and accounting policies.

4.12 Our work included interviews with management and staff, as well as a review of systems, processes, agreements, policies and other documentation. Criteria were developed to assist in the planning and performance of the assignment. The criteria used in our review of general computer environment controls were derived from the *Information Technology Control Guidelines* of the Canadian Institute of Chartered Accountants. Other criteria used were specifically developed for this assignment. The criteria were discussed with senior management of the Department and accepted as appropriate.

PRINCIPAL FINDINGS

General Computer Environment Controls

4.13 Our objective in this section of the assignment was to review control over the general computer environment within the Department of Community Services. Our review of controls included those relating to risk management, information technology planning, operations, security, change management, and end-user computing, as well as disaster recovery and business continuity planning. We noted areas where control is adequate, but also identified significant control weaknesses. The seriousness of the weaknesses and absence of adequate compensating controls led us to conclude control over the Department's general computer environment is generally inadequate.

4.14 Control over the Department's general computer environment is adequate in certain areas, including the following.

- Roles and responsibilities related to information technology are clearly defined and communicated.
- System infrastructure is housed in an appropriately-controlled environment.
- Controls are in place to ensure changes made to system applications are appropriately approved.
- There are processes to ensure users of Department computers are aware of significant security and other risks and take measures to address them.
- There is a formal planning and monitoring process for controlling information technology projects.

4.15 Risk management and information technology policy - During our review, we noted the Information Technology Services (ITS) section relies on the government's Corporate Information Technology Organization in certain areas such as information technology security, disaster recovery and business continuity planning. This is appropriate because many areas of risk management are the responsibility of the Corporate Information Technology Organization. However, some areas of information technology risk management, such as computer access and application controls, are the responsibility of the Department. These have not been formally identified and evaluated by the Department. We were advised by the Department that these areas of information technology risk management will be addressed by a business continuity planning initiative currently underway. We noted the Department is in the process of creating a risk register which identifies and evaluates risks. This register also notes the strategies in place to address risks. It is very important that the Department identify and control all significant information technology risks that could lead to losses of public funds or government assets, interruptions in service delivery and/or failure to protect the privacy of personal information. We encourage the Department to complete this process as soon as possible.

4.16 Management indicated they have a number of informal policies and procedures, such as requirements to complete project risk analyses, regularly review service level agreements and make timely changes to user access rights. We believe having informal, undocumented policies increases the risk of important processes not occurring as intended.

Recommendation 4.1

We recommend the Department formally document significant policies and procedures relating to the use of information technology within the Department.

4.17 Planning - The planning process within ITS is driven by the Department's overall business planning process. ITS contributes to the Department's plan and prepares project-specific plans, but does not prepare formal annual plans for its operations. The operations of ITS are extensive, involve high-risk processes and are critical to the success of the Department, as well as the other entities to which information technology services are provided. We believe operations of such magnitude and importance should prepare annual operational plans in order to control risks and ensure progress occurs as intended.

4.18 An information technology strategic plan was prepared in 2000. Management indicated it is still being applied to the Department's operations. However, technology has progressed significantly in the last six years and we believe the plan should be updated.

Recommendation 4.2

We recommend the Department review and update its information technology strategic plan to ensure it reflects changes in information technology and continues to meet Department and user needs. We also recommend an annual business or operational plan be prepared for the Information Technology Services section.

4.19 Service agreements and performance - ITS has service level agreements with the Department of Service Nova Scotia and Municipal Relations, the Children's Aid Societies, the regional housing authorities, and other divisions within the Department of Community Services. The objective of these agreements is to ensure user systems are operating in accordance with agreed upon standards. These agreements serve as the primary measure of performance for ITS. Senior management within ITS meet on a regular basis to discuss operations, projects and any issues identified by clients or ITS staff. ITS also compiles information on services provided. ITS uses these meetings and information on services provided as the basis upon which to assess the section's performance. While these measures are useful, we believe that more formal monitoring and reporting of performance would provide better information. In our view, informal assessments and reliance on user concerns and complaints as the primary measures of performance are inadequate for fully assessing the performance of the section.

Recommendation 4.3

We recommend the Department develop performance outcomes, measures and targets for its

Information Technology Services section and assess the performance of the section against these targets on a regular and timely basis.

4.20 Access controls - Proper control over information technology includes controlling access to computers through the use of passwords and limiting computer access rights to only those necessary for staff to effectively fulfill their specific responsibilities. Unrestricted or inappropriate access to systems and data can increase the risk of unauthorized transactions or program changes, leading to financial losses and/or interruptions in services and programs administered by the Department.

4.21 We reviewed access rights for seventeen individuals who had left the Department. We found nine (53%) of these individuals still had computer access rights at the time of our review. Five had network access, three had access to the income assistance program and one had access to both. Access to both the network and income assistance program represents a significantly higher risk. ITS management stated that access change documentation is often not received in a timely manner.

4.22 Our audit identified segregation of duties issues within the Department. We noted certain accounting staff could initiate an ad hoc payment to an existing income assistance client. These individuals also have access to accounting records and are responsible for income assistance payments and bank reconciliations. Staff informed us that these access rights are not required to fulfill their position responsibilities. The ability to both initiate and account for payments is inappropriate from a control standpoint because it provides opportunity to initiate a fraudulent transaction and conceal or delete it from the books of account. We did not identify any compensating controls to mitigate this risk. Management advised us that access rights are being updated to address our concern.

4.23 We also identified five individuals who share the same password to access a computer used in the processing of electronic funds transfers. Management advised us that, for technical reasons, it is necessary to share this password. However, computer logs are not used to monitor user activity related to this computer system. Use of this computer needs to be strictly monitored and controlled in order to prevent unauthorized changes which could result in financial losses or other negative consequences to the Department.

Recommendation 4.4

We recommend the Department review user access rights to ensure they are limited to those necessary to effectively fulfill assigned job responsibilities. The Department should also ensure documentation related to access rights changes is completed and submitted to the Information Technology Services section on a timely basis. We further recommend that the Department monitor user activity on critical computer systems.

4.24 Recovery planning - Recovery planning is a critical component of any significant information technology operation. We noted that the Department has processes for systematic recovery if data and processing capabilities are lost, including use of offsite resources if needed. However, the Department has not formally documented or tested its recovery plans. We believe recovery planning should be formalized in the Department's information technology policies (see Recommendation 4.1) and risk management strategy (see paragraph 4.15).

Electronic Funds Transfer Controls

4.25 The objective for our audit of electronic funds transfers (EFT) for the Employment Support and Income Assistance (ESIA) program was to assess the adequacy of controls used to ensure electronic funds transfers are complete, accurate, properly approved and for authorized purposes. We noted some appropriate controls in this area. However, we also identified weaknesses significant enough to lead us to conclude control over electronic funds transfers is generally inadequate.

4.26 The Department of Community Services provides financial assistance to persons eligible under the Employment Support and Income Assistance Act (see December 2005 Auditor General's Report - Chapter 6). Income assistance recipients can elect to have payments made by cheque or direct deposit. Direct deposit payments are made once a month by way of electronic funds transfers. During the month of March 2006, the Department issued 45,553 payments totaling $31.6 million of which 11,990 payments totaling $7.2 million were directly deposited to recipient bank accounts.

4.27 We identified the following adequate controls relating to electronic funds transfers in the Employment Support and Income Assistance program.

- Records used by the bank to process electronic payments are reconciled with the payment records of the Department.
- Electronic files sent to the bank for processing electronic payments are encrypted.
- There is appropriate physical security provided for the computer used to process electronic funds transfers.
- Persons responsible for initiating and accounting for EFT payments have no access to the computer used to process electronic funds transfers.
- We did not identify any errors or unreconciled items in the eight EFT reconciliations we examined.

4.28 Computer edit controls - We noted that the creation and transfer of direct deposit information to the bank making the deposit is automated. The Employment Support and Income Assistance (ESIA) system generates a payment list which details the income assistance payments to be made. This list is transformed by the

ESIA system into an EFT file, which is automatically transmitted to the EFT server for transfer to the bank for payment. Before payments are made, the bank sends a control statement back to the Department so the Department can reconcile the bank's totals to the ESIA system totals.

4.29 However, we found that there are no computerized edit checks or review for unusual balances before the file is sent to the bank. In addition, there is no process to ensure the reconciliation of control totals has been completed before the bank processes payments. The bank automatically processes payments three days after a control statement is sent to the Department, whether or not the reconciliation has occurred. This weakness is exacerbated by the system deficiencies identified in paragraphs 4.21 and 4.22.

Recommendation 4.5

We recommend the Department implement computerized edit checks of electronic funds transfer data and a process to ensure reconciliations occur before the bank makes income assistance payments.

4.30 In paragraphs 4.21 to 4.23 we identified weaknesses related to control over who can access the systems used to create and process EFTs. The related risks are significantly exacerbated by the lack of a programmed dollar limit on EFT payment transactions. If a person could manage to access the system for purposes of initiating a fraudulent payment, there is no limit on how large this transaction and the resulting loss to the Department could be.

Recommendation 4.6

We recommend the Department modify its electronic funds transfer systems to set a limit on the size of individual electronic funds transfer payments.

4.31 Bank reconciliations - Our examination of bank reconciliations identified unreconciled differences and long outstanding cheques for which explanations were not provided. Neither of these relate to EFTs, but represent, nonetheless, significant control weaknesses. Bank reconciliations are critical for ensuring all bank transactions are properly recorded. We noted reconciliations were not signed by the preparer or the reviewer. Management advised us that reconciliations are reviewed and approved but were not signed due to the unreconciled items. In the absence of a documented review and approval process, we were unable to determine whether the review and approval process was occurring as described to us. Documentation of the process would help ensure bank reconciliations are properly performed according to schedule, reviewed appropriately and that all appropriate adjustments are made on a timely basis. We believe unreconciled differences and long outstanding cheques should be fully resolved.

Recommendation 4.7

We recommend the Department ensure the bank account is fully reconciled. In addition, reconciliations should be reviewed and approved and there should be documented evidence of the review and approval.

4.32 Policies and procedures – Our audit found there are no government-wide or Departmental policies or procedures to guide staff involved in electronic funds transfers. We noted Community Services has only partially documented its EFT process.

Recommendation 4.8

We recommend the Department formally document all policies and procedures related to its electronic funds transfers.

4.33 Data security - EFT transactions for the Department are administered in accordance with an agreement between its bank and the Department of Finance. The Department of Community Services does not have an understanding of the controls in place at the bank to protect the integrity and use of the Department's EFT data. For example, there is no formal agreement on how the bank should protect the privacy of personal information related to income assistance clients. There is no detailed understanding of the level of security provided by the encryption applications used by the bank to transfer EFT files from the Department to the bank. We believe the Department should discuss control over the privacy and security of EFT data with the bank and enter into an agreement which results in an acceptable level of risk to the Department.

Recommendation 4.9

We recommend the Department or government enter into a formal agreement with the bank respecting the control the bank is expected to apply to electronic funds transfer data for income assistance recipients.

4.34 The bank is provided with a list of Department staff authorized to communicate on behalf of the Department on banking matters. We found that the list is not current. Some individuals on the list have since retired. We advised the Department to update its authorized contact list.

Information Technology Purchases

4.35 The objective of our audit of information technology purchases was to assess whether purchases are properly approved, accurately recorded and in compliance with Provincial procurement and accounting policies. We concluded purchases are properly approved, accurately recorded and in compliance with the policies. We also noted an opportunity to improve the efficiency of the purchasing process.

4.36 Our audit work included an examination of fifty purchase transactions. Each of these transactions was properly approved and accurately recorded in accordance with government accounting policies. Forty-nine of the purchases tested (98%) were in compliance with the Provincial procurement policy. Three quotes were not obtained for one purchase, as required by the policy.

4.37 Our examination identified an opportunity to improve the efficiency of the purchasing process by reducing the number of approvals needed. We found there can be as many as seven levels of approval, including the Minister's authorization. Management indicated the current number of approvals adds considerable time to the purchasing process. Seven levels of approval may not be required for effective control over the information technology purchasing process.

Recommendation 4.10

We recommend the Department examine its information technology purchase approval process and evaluate the necessity of having the current number of approvals.

CONCLUDING REMARKS

4.38 Our work on selected internal controls identified some very serious control weaknesses. These include inadequate access controls, inappropriate segregation of duties, ineffective bank reconciliation procedures and inadequate review and approval processes. Certain control weaknesses identified in this chapter pose a significant risk of financial loss or other negative consequences, either through fraudulent actions or error. We strongly encourage the Department to prioritize the control weaknesses identified in this chapter and address those which pose a significant risk as soon as possible.

DEPARTMENT OF COMMUNITY SERVICES' RESPONSE

The Department appreciates the opportunity to respond to the findings of the Auditor General report on the "Information Technology and Financial Controls". The Department acknowledges the positive findings in the report, and will be implementing system control improvements in areas identified in the report.

While some control improvements are best left until the impending strategic implementation of the new Integrated Case Management (ICM) system, several control improvements are being considered in the meantime.

Thank you for your feedback.