4 Education and Early Childhood Development: iNSchool Student Information System

Summary

The iNSchool student information system does not fully protect the confidentiality, integrity and availability of information on students in the public school system.

We identified security weaknesses with the iNSchool system. We chose three school boards to test and exploited those weaknesses to gain unauthorized access to confidential student information such as grades, medical conditions, health card numbers, parental or guardian contact information and home addresses. Unauthorized access to student information presents very serious risks, including unauthorized changes to data (e.g., grades, allergy warnings), student safety by having contact information available, and identity theft. Before we wrote this report, the iNSchool project team fixed the critical security issues that enabled us to gain access to the student accounts.

Government systems containing personal information are required to have a privacy impact assessment prepared to evaluate and mitigate privacy risks, such as the ones we found in iNSchool. An assessment was started for the system, but it was not completed. Important components of the assessment, such as strategies to mitigate privacy risk, remain unfinished.

The Department of Education and Early Childhood Development has implemented controls to protect the network and physical equipment that host iNSchool. These include intrusion detection systems, firewalls, performance and capacity monitoring, incident management (e.g., responding to hacking attempts), offsite back up of critical data and measures against environmental threats (e.g., fire). We made recommendations to enhance these processes to help ensure continuous availability of data and protect against unauthorized access to systems.

The development of the iNSchool system was aided by an appropriate governance structure with involvement from users and other stakeholders. Reasonable project management practices were used throughout the project lifecycle.

The design requirements of the new system appropriately considered the needs of its users and the concept of value for money. Government's procurement rules were followed in selecting the iNSchool system.

4 Education and Early Childhood Development: iNSchool Student Information System

Background

4.1 The Department of Education and Early Childhood Development and the school boards implemented a suite of applications called the Nova Scotia Student Information System, commonly referred to as iNSchool. It provides access to up-to-date information on students, schools and programs in the public education system. Parents, students, teachers and school administrators can access student marks, performance plans, attendance records, assignment due dates, and school announcements, all through a web-based interface.

4.2 Prior to the implementation of iNSchool, school boards managed their own student information systems and processes. One goal of iNSchool is to provide consistent public school student data throughout the Province on a timelier basis.

4.3 The iNSchool suite of applications includes the following.

- PowerSchool: This application manages core student information, such as report cards, demographics and schedules. It includes an internet-accessible portal enabling parents and students to see current information on matters such as attendance, grades, assignments, teacher's comments, and upcoming school events. The system maintains records for approximately 120,000 students.

- TIENET: This application manages extended services for students with additional needs, such as individual program plans and information from the SchoolsPlus program, which provides additional supports and services to students.

- Learning Management and Reporting System: The scope of the Learning Management and Reporting Project is to support the learning and teaching function with a complete and integrated solution. It includes curriculum and resource management; instruction, classroom assessments and evaluation; Provincial and common assessments; and teacher professional learning. This application is expected to be implemented at a later date.

4.4 Implementation of iNSchool was managed by a project team which consists of the Department of Education and Early Childhood Development's Information Technology Services division, school board representatives and contract employees.

4.5 Some schools in all school boards were using the system by September 2010, and all schools throughout the Province used iNSchool by September 2013. Implementation rates varied because of differences in size of the school boards, legacy systems in place that required data conversion, and French translation requirements.

4.6 The capital cost of implementing PowerSchool and TIENET was budgeted at $12.75 million. Actual costs as of March 31, 2013 totaled $12.5 million, leaving $0.25 million for remaining costs.

Audit Objectives and Scope

4.7 In fall 2013, we completed an audit of the Nova Scotia Student Information System (iNSchool). The goal of the audit was to determine whether appropriate processes were used in the planning, design, procurement and implementation of the system, and whether the system and information it contains are adequately controlled.

4.8 The detailed objectives of the audit were to assess whether the Department of Education and Early Childhood Development and the school boards:

- implemented an electronic student information system with sufficient controls in place to protect the confidentiality, integrity and availability of Nova Scotia's public school students' information;
- implemented adequate procedures to monitor and support the information needs of users throughout the iNSchool system; and
- followed procurement and implementation processes during the iNSchool project that ensured the system was designed to meet the needs of its users and consider value for money.

4.9 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 Education and Early Childhood Development senior management.

4.10 The audit was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards adopted by the Chartered Professional Accountants of Canada. Audit fieldwork was performed between June and October 2013 on project management-related activities which occurred

during the period from 2009 through 2013. Technical aspects of systems were assessed at various points in time between July and December of 2013.

Significant Audit Observations

Information Security and Protection

Conclusions and summary of observations

Security over student information in the iNSchool system needs improvement. The security settings of iNSchool and its hosting databases and operating systems need to be better configured to prevent unauthorized access. We were able to gain unauthorized access to many iNSchool user accounts and student information contained in them. We found several appropriate network controls, but we found security weaknesses at the operating system, database and application levels. System access requests are not documented and there is no evidence of periodic reviews of accounts for dormancy. The privacy impact assessment for iNSchool has not been finalized. Important components of the assessment related to the protection of data have not been completed. An IT disaster recovery plan does not exist to help restore iNSchool and supporting infrastructure in the event of a disaster. We have recommended improvements to manage and protect the physical environment supporting the systems that host iNSchool.

4.11 *Security management and controls* – Sensitive information stored in computer systems needs protection against unauthorized changes and disclosure. Best practices call for a security management process for important IT systems that includes establishing and maintaining roles and responsibilities, policies, standards and procedures. Good security management also includes system security monitoring, periodic testing, and implementing corrective actions for identified security weaknesses.

4.12 Each school board has its own dedicated copy of the iNSchool application running on servers that are managed and supported by the Department. The servers contain the operating systems necessary to run the iNSchool application and the databases which store iNSchool data. The school boards participate in the day-to-day administration of the application system and are responsible for functions such as managing user access and providing user support.

4.13 *Network controls* – The servers that run the iNSchool application are located on the Department's internal network. The Department has implemented safeguards on this network to help protect the iNSchool servers from being attacked or compromised by other Department servers that are also part of

the internal network and used in different program areas. Safeguards include multiple firewalls and intrusion detection systems which are monitored by staff.

4.14 *Operating system and database controls* – In the event network controls fail, the operating systems that run the iNSchool application and the databases that store its data need strong controls to prevent unauthorized access to students' personal information. Our audit identified weaknesses in operating system and database controls supporting the iNSchool application. These weaknesses included a lack of measures to force accounts to have strong passwords and insufficient logging of account activity.

4.15 *Application controls* – Users, including teachers and school administrators, access iNSchool from a website which is generally accessible to anyone over the Internet. This form of access increases risk and, accordingly, increases the need for strong access controls. We found that each school board administers its own password and account settings and that some of those settings were too weak to adequately prevent unauthorized access through the Internet. In addition, an analysis of PowerSchool system logs that track login attempts showed several examples that had the characteristics of individuals attempting to gain unauthorized access to the application. This further emphasizes the need to maintain strong username and password settings.

4.16 We attempted to gain access to the iNSchool data of three school boards by exploiting weak password controls and account settings. We were able to gain unauthorized access to iNSchool user accounts. The accounts accessed provided us with the ability to identify and target administrator accounts. As a result, we gained access to all students' information in two school boards and access to a large number of students' information in the third board.

4.17 Student information available to us as part of this exercise included:

- birthdates;
- medical information;
- home addresses;
- health card numbers;
- locker numbers and combinations;
- grades;
- iNSchool account information; and
- email addresses (student and parents).

4.18 Unauthorized access to student information presents very serious risks, including unauthorized changes to data (e.g., grades, allergy warnings), student safety by having contact information available, and identity theft.

4.19 After we informed the iNSchool project team of our findings, they added additional security controls in the PowerSchool application and addressed configuration and account weaknesses for higher-risk user accounts. Further security upgrades to remaining user accounts are expected.

Recommendation 4.1
The Department of Education and Early Childhood Development and school boards should implement consistent, strong controls on the operating systems, databases and applications of iNSchool, including enforcement of strong passwords and account settings.

Department of Education and Early Childhood Development Response:
There have not been any known compromises of iNSchool since it was first implemented. Nevertheless, the Department agrees with this recommendation, and has upgraded the PowerSchool application and key user accounts to meet or exceed provincial standards on account management. The Department will complete upgrades to remaining user accounts in the near future.

4.20 *User account management* – School boards are responsible for providing access to the Power School and TIENET applications. New users are assigned a username, password and access to the specific system modules needed to perform their jobs. Each school board has its own processes for accepting requests for access including by email, phone, in person and through a central electronic tracking system. These requests are not always documented and retained for future review. Maintaining documentation of requests for system access, along with the specific system permissions granted, is important as it enables the administrator to track and manage access requests, as well as helping to ensure only authorized individuals receive access.

Recommendation 4.2
The Department of Education and Early Childhood Development should work with the school boards to develop a process that tracks requests for, and changes to, access to iNSchool.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation. Such a process is in place in some school boards. The Department will work with the remaining school boards to develop a process that tracks requests for and changes to access to iNSchool.

4.21 School administrators are responsible for disabling unneeded user accounts. All school boards told us that a periodic review is performed to ensure all existing user accounts are still needed. However, we found no documented evidence of this process.

Recommendation 4.3
The Department of Education and Early Childhood Development should work with the school boards to develop a process that records the outcome of the periodic review of accounts and the details of the resulting disabled accounts.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation and will work with the school boards to develop a process that records the outcome of the periodic review of accounts and the details of the resulting disabled accounts.

4.22 *Privacy impact assessment* – The Department of Education and Early Childhood Development privacy policy states:

> *"The Department of Education shall complete a privacy impact assessment for any new program or service, or for a significant change to a program or service, which involves the collection, use or disclosure of personal information, as per the template maintained by the Information Access and Privacy Office, Department of Justice."*

4.23 A privacy impact assessment is a thorough analysis of potential impacts on privacy and a consideration of measures to eliminate or mitigate negative impacts. This due diligence exercise ensures a system owner identifies and addresses potential privacy risks that may occur as a result of a system's design and operation.

4.24 The iNSchool project team prepared a draft privacy impact assessment. However, at the time of our audit, this document was not completed. The unfinished assessment did not address strategies to mitigate privacy risk, such as procedures to track and monitor the system for unauthorized use. This is a critical component that should have been documented and approved before the system was made available for use.

Recommendation 4.4
The Department of Education and Early Childhood Development should complete and approve a privacy impact assessment for iNSchool. Processes should be developed and implemented to address any risks identified in the assessment.

Department of Education and Early Childhood Development Response:
The Privacy Impact Assessment was substantially completed during implementation of the system. The Department agrees with the recommendation and will finish the document and have it formally approved.

4.25 *Continuous service* – In the event of a disaster, organizations need to minimize the interruption to key business functions should information technology become unavailable. It is important to regularly back up system data offsite

and to have and test a comprehensive disaster recovery plan outlining how and where systems will be restored in order to have a timely recovery of the organization's operations.

4.26 The Department of Education and Early Childhood Development maintains backups of iNSchool data offsite and has administrative guides for restoring and configuring the systems. However, it does not have a disaster recovery plan.

Recommendation 4.5
The Department of Education and Early Childhood Development should prepare a disaster recovery plan that includes the iNSchool system. The Department should provide training and perform testing on the disaster recovery plan.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation and will prepare a disaster recovery plan that includes the iNSchool systems.

4.27 *Physical environment* – Organizations implement safeguards to physically protect their computer systems. Risks to the physical security of systems come from both people (e.g., accidents or vandalism) and environmental factors (e.g., water, heat or electrical interruption), each of which could cause significant damage to information technology systems and possibly interrupt the organization's core services and operations.

4.28 The private-sector building owner is responsible for the heating and cooling, back-up power, and physical security for the building that houses the iNSchool servers. We found that appropriate infrastructure and controls are in place to protect the server room. This includes an uninterrupted power supply, environmental controls (e.g., controlling heat and humidity), fire suppression, and restricted access to the room. The server room also has a backup generator. However, the generator was not tested with a full electrical load during its last maintenance inspection to ensure it can support the full power requirements of the server room.

Recommendation 4.6
The Department of Education and Early Childhood Development should validate with the building owner that generator maintenance is performed as scheduled, including a full load test.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation and has made arrangements with the building owner to: i) obtain a copy of the maintenance report when scheduled generator maintenance is performed; and ii) obtain a copy of the test results report each time a full load test is performed. Copies of the most recent maintenance and load test results reports have been received.

4.29 We also noted that the position of the server room in the building puts the systems at some risk of water damage. Therefore, there should be a water sensor installed on the floor inside the server room to assist in early detection of water leakage.

Recommendation 4.7
The Department of Education and Early Childhood Development should install a water sensor in its server room.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation and will have a water sensor installed in the server room.

System Procurement and Implementation

Conclusions and summary of observations

A reasonable project management process was used to guide the implementation of the iNSchool system. User needs were the basis for determining system requirements and ultimately selecting the preferred solution. Provincial procurement practices were followed. Appropriate levels of management and users were part of the governance structure of the project. Stakeholders were kept informed by way of regular status reports and meetings, and had forums available to provide input throughout the project. However, security considerations were not adequately addressed before implementation.

4.30 *Project management* – Effective project management reduces the risk of unexpected costs, improves communications with stakeholders, and increases the value and quality of the end product. The success of planning, implementing and maintaining a new information system is reliant on the project management framework employed. A reasonable project management process was used to guide the implementation of the iNSchool system. The iNSchool project management framework addressed project governance, procurement, timeline and budget management, as well as system testing and training. Many stakeholders were involved throughout the project. However, as noted in the Information Security and Protection section above, security of the operating systems, databases, and PowerSchool applications were not adequately addressed as part of project management or the implementation process.

4.31 *Governance structure* – Appropriate levels of management and system users were part of the governance structure of the project. Strategic planning was facilitated through an Executive Steering Committee, a Management Steering Committee and a Project Managers Committee. Project organization groups included a Provincial Coordination Team, as well as functional and technical

forums with representatives from the school boards and the people who would regularly use the new system. Terms of reference were created and activities of the various committees were evident from regular status reports and meeting minutes. Stakeholder involvement was consistent throughout the project.

4.32 *Procurement* – We reviewed the procurement processes for the iNSchool system and determined that vendor selection procedures were in accordance with Provincial standards. The iNSchool project team worked with Government's procurement services office and followed an appropriate procurement strategy. There was a formal process to develop system requirements and score vendors against those requirements. A committee was formed with representation from the school boards and the Department of Education and Early Childhood Development to negotiate a fair and reasonable contract. Legal guidance was provided by the Department of Justice.

4.33 *User needs* – An appropriate process was used to select the best product to meet the needs of the users. The iNSchool system requirements were defined by its users. They described the processes followed before iNSchool, which then became the basis for what the new system must accomplish. Potential products were evaluated against these requirements. Users participated in feasibility studies and completed questionnaires during the product selection phase.

4.34 *Budget management* – An effective budget management process fosters partnership between business stakeholders; promotes effective and efficient use of IT resources; and provides transparency and accountability. A review of project documentation showed that the iNSchool project had reasonable processes in place to develop the budget with stakeholder input. Stakeholders were notified of how the project was doing against its budget through project status reports and at status meetings.

4.35 *Testing and change management* – The iNSchool project team executed an appropriate testing strategy that included a dedicated testing environment (a system isolated from live systems) and user involvement. Changes to processes and design are not unusual during the implementation of a new system and such changes need to be carefully managed. Changes for the iNSchool system were approved and tracked throughout its implementation.

4.36 *User support* – Training plans were developed in conjunction with the system vendors to meet the needs of all users. The project team and vendor were responsible for developing the training content and the vendor was responsible for delivery of initial training. The delivery of training was monitored and tracked within each school board. A website was created to store training and support materials. Surveys were administered to obtain and respond to feedback from users on training matters.

4.37 Once a project is fully implemented, ongoing support is needed. This should include documentation and communication of policies, roles, responsibilities, standards and guidelines with respect to ongoing support. This was not complete at the time fieldwork was conducted, but had been started. We encouraged the Department to continue its efforts.

System Monitoring and Usage

Conclusions and summary of observations

Reasonable processes were in place to monitor and evaluate system performance during the implementation of iNSchool. Department of Education and Early Childhood Development staff do not have documented performance monitoring procedures that they can refer to. There were processes at the school, board, department and vendor levels to address incidents with the iNSchool application. Common problems and incidents were reported and discussed at committee meetings. There is no problem management process to identify and respond to the root causes of system incidents. iNSchool is available for use at all school boards and there are indications that it is being used regularly by teachers and school administrators.

4.38 *System monitoring* – The ability of iNSchool to meet capacity and performance requirements was assessed as part of the procurement process. During the implementation phase, management monitored system performance. The infrastructure which supports iNSchool (network, servers and databases) was also continuously monitored with the assistance of vendor-supplied monitoring software.

4.39 The performance of networking hardware and servers hosting the iNSchool application should continue to be monitored and evaluated now that iNSchool is fully operational. The Department of Education and Early Childhood Development does not have documented procedures indicating which networking devices (e.g., intrusion detection systems, switches, routers, firewalls) and which servers and their metrics (e.g., CPU performance, memory usage, hard drive capacity) should be monitored. Other considerations include what monitoring should cover, frequency, and what action to take when potential performance or capacity issues are identified. Documentation of the procedures provides reference for staff as they ensure the system continues to maximize value and meets the needs of users.

Recommendation 4.8
The Department of Education and Early Childhood Development should document and implement a performance management process that includes procedures to indicate which networking hardware, servers and metrics should be monitored, how frequently it should occur, what staff should look for, and steps to take if incidents are identified.

Department of Education and Early Childhood Development Response:
The Department uses industry standard monitoring software which contains an inventory of the devices monitored and the schedule. The inventory and schedule can be extracted when needed. The Department agrees with this recommendation and will document the existing process.

4.40 *Incident and problem management* – Incident management is the process of identifying and resolving IT-related events that have a negative impact on an organization's computer systems. This process focuses on fixing the immediate issue. Problem management is the process of investigating why such incidents occur and attempting to fix the underlying issue that caused the incidents. If these two processes are not in place and operating effectively, there could be extended interruption of IT systems.

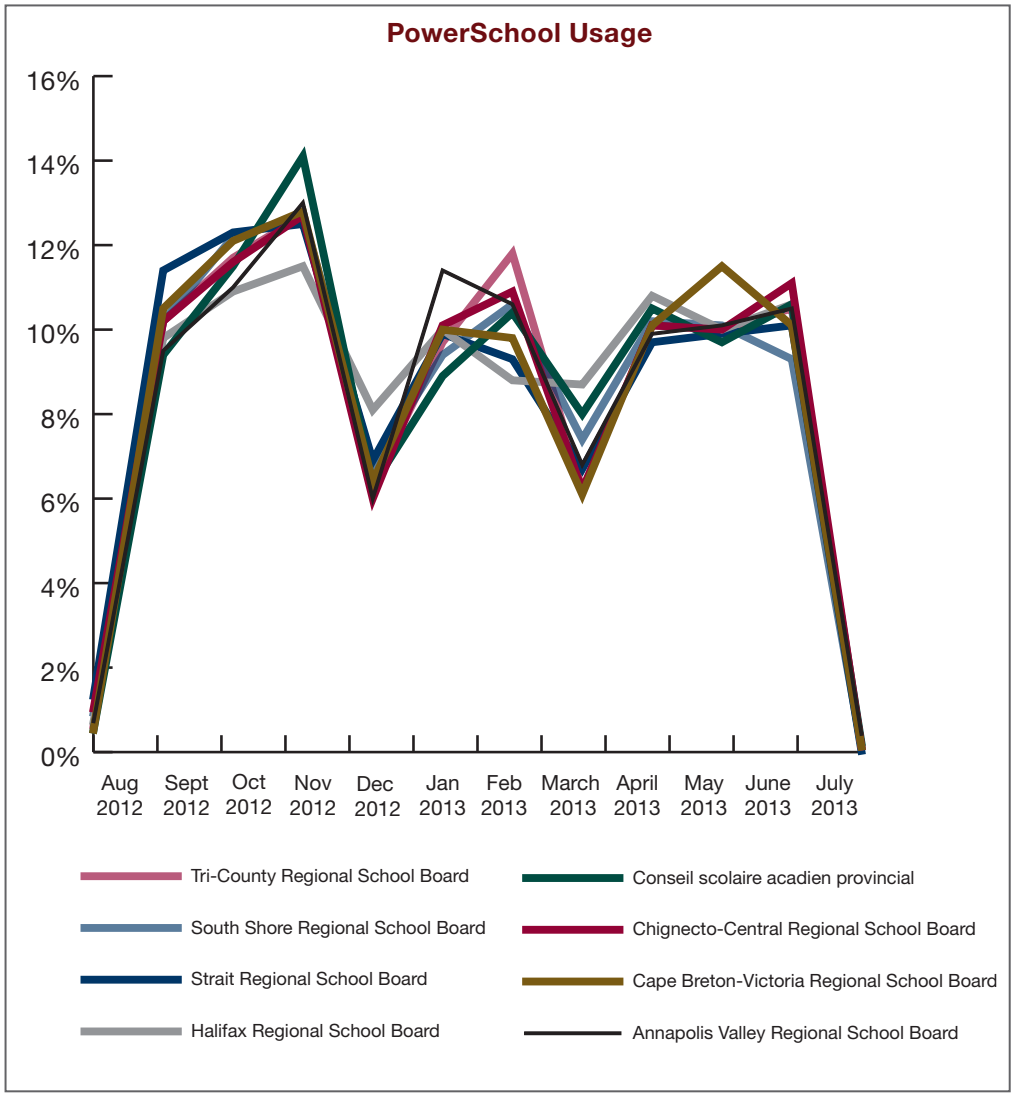
4.41 System incidents were regularly discussed at status meetings during the implementation of iNSchool. Each board was represented on the project management team and had opportunity to discuss common incidents. These members still meet frequently and recurring issues can be discussed to determine if there are any commonalities.

4.42 Issues identified are recorded in the Department of Education and Early Childhood Development's ticketing system. Issues that cannot be fixed by the Department are sent to the vendor's ticketing system for review and possible resolution. School boards are also able to submit a system incident to the Department's ticketing system if it cannot be resolved at the school board level. However, not all school boards document the incidents that they have addressed without vendor assistance or discussions with the project management team. This makes it difficult to track, manage and resolve incidents, or assess whether recurring incidents are a result of a greater problem. There should be a problem management process that describes how all issues should be recorded and monitored over time across all school boards, to capture those incidents which did not require Department, vendor or project management team assistance.

Recommendation 4.9
The Department of Education and Early Childhood Development should work with the school boards to document and track iNSchool system incidents. Incidents should be analyzed to identify and respond to their root causes.

Department of Education and Early Childhood Development Response:
The Department agrees with this recommendation and will work with school boards who are not documenting all incidents. The Department will continue to work with school boards to analyze incidents and respond to their root causes.

4.43 *System usage* – We analyzed iNSchool login data to determine if the system is generally being used on a regular basis by teachers and school administrators throughout the public school system. The chart below shows that usage was consistent among the boards for the 2012-13 school year. It aligns with the cyclical nature of the typical school year calendar. For example, all school boards had their highest login rates during the month of November, which coincides with report card preparation. The lowest login rates occurred in July, which reflects the summer vacation period.



Department of Education and Early Childhood Development
Additional Comments

The Department received value from the audit and was pleased with the process, and the professionalism and quality of staff. We addressed the most significant recommendations immediately, and will deal with the others as indicated in the Department's response. As this report shows, the iNSchool program was delivered on time, on-budget, and with the necessary rigour to ensure that it meets the quality expectations of the public school system.