Office of the Auditor General
500 - 330 Portage Avenue
Winnipeg, Manitoba R3C 0C4

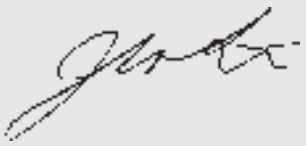
March 2004

The Honourable George Hickes
Speaker of the House
Room 244, Legislative Building
Winnipeg, Manitoba
R3C 0V8

Dear Sir:

I have the honour to transmit herewith my Information Technology Reports to be laid before Members of the Legislative Assembly in accordance with the provisions of Section 28 of The Auditor General Act.

Respectfully submitted,



Jon W. Singleton, CA•CISA
Auditor General

TABLE OF CONTENTS

REFLECTIONS OF THE AUDITOR GENERAL

Those responsible for information technology decision-making in the public sector face the challenge of optimizing and governing the use of IT within allocated funding. A key in ensuring that IT aligns with the objectives of entities is the development and reference to an IT Strategic Plan that is well coordinated with the overall strategies of the organization. At the time of our work, Red River College was well situated in this regard. However, the Province of Manitoba needs to take steps to clarify its IT Governance practices and to develop overall IT Strategic Plan and IT Performance Measurement System.

Red River College Information Technology Audit

With this report, we have completed our review of information technology (IT) in Manitoba's Community Colleges. As with Keewatin and Assiniboine Community Colleges, the implementation of effective IT at Red River College (College) plays an increasingly significant role in supporting the effective and efficient administration of the College and enhancing the learning experience of students.

We believe that, overall, the College has done a good job of managing IT resources. However, our audit identified a number of areas for improvement including:

- developing performance indicators for IT;
- regularly gauging user satisfaction with IT systems and services;
- strengthening IT purchasing and tendering practices; and
- taking further actions to protect computer networks.

The comments from the College have been incorporated into this report. It is encouraging that the College has already addressed a number of our recommendations, including the development of a new IT purchasing policy.

While Red River College is significantly larger than both Keewatin Community College and Assiniboine Community College, we found that they each faced similar challenges and threats regarding the effective and efficient delivery of IT services and the need for improved systems and network security. These common needs provide an opportunity for the Colleges to work together to find common solutions.

The ongoing challenge for both the Province and the Colleges will be finding the financial resources to adequately address the rapid changes in technology to ensure that College students continue to meet the needs of tomorrow's employers.

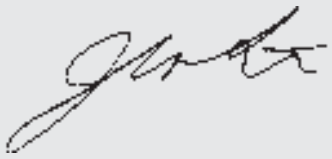
A Review of the Information Technology Organization in the Province of Manitoba

In this report we stressed the importance of the Province ensuring that the Information Technology organizational structure be aligned with government objectives and strategic plans, and noted that a strong IT governance structure, with strong and defined leadership authority was important to ensure that employees of the province function effectively. As well, we noted that without a performance measurement system and an overall quality assurance system in place, there was a risk that IT objectives would not be met. The Province has indicated that steps are being taken to make improvements consistent with our recommendations.

A Review of Computer Security Incident Response Capability in the Province of Manitoba

In this report we looked at the Province's capability of properly responding to computer security incidents in Departments.

We concluded that the Province is capable of properly responding to computer security incidents involving the computer environment managed by a service provider for Departments or the computer application servers managed by those Departments. However, we did identify some opportunities for operational improvement. The Office of Information Technology concurred with our recommendations.



Jon W. Singleton, CA•CISA

RED RIVER COLLEGE OF APPLIED ARTS, SCIENCE AND TECHNOLOGY
IT AUDIT

1.0 Executive Summary

As the last chapter of our review of information technology (IT) in Manitoba's Community Colleges, we conducted a value-for-money audit of Red River College's (College) investment in IT. IT represents a significant annual investment of College resources, and is a key success factor in the College's achievement of its mission and goals. Similar audits have been completed and reports issued on Keewatin Community College and Assiniboine Community College.

The objective of our audit was to answer the following four questions:

1. Is the College making sufficient progress in achieving its information technology objective?
2. Are information technology systems and services adequately meeting the needs of users?
3. Are information technology purchases made with due regard for economy and effectiveness?
4. Is the College taking appropriate action to minimize the risk of unauthorized access to its computer networks?

Audit procedures were performed during the period December 2001 through June 2002, and included examining available records and conducting interviews with College officials, administrative staff, and faculty.

The College delivers over 110 diploma, certificate, and apprenticeship programs in the fields of applied arts and sciences, business, community services, developmental education, health, trades, and technology. College programs are delivered in a number of locations in Winnipeg and Southern Manitoba. The expenditure budget for 2001/02 was $81.0 million. Revenues included provincial grants of $47.0 million.

For this value-for-money audit, we focused primarily on the Computer Services (CS) Department. Under the leadership of the Chief Technology Officer, the CS Department is responsible for college-wide information technology services including planning, application development, database administration, hardware support, operations support, communications support, application support, corporate systems training, and special projects. The Chief Technology Officer manages a budget of approximately $3 million, and a complement of 37 staff positions.

In summary, we concluded that:

- The College reported significant progress in completing most of the 2000/01 actions associated with the strategies flowing from the IT Objective #6 (integrate Information Technology in the delivery, operation, and management of all College programs and services) in the College's Strategic Plan (Figure 5). However, because the College had not developed sufficient performance measures for IT, we could not assess the degree to which the Objective was being met.
- The majority of users surveyed or interviewed indicated that they were generally satisfied with IT systems and services. Opportunities still exist for the College to regularly gauge whether user needs are being

adequately addressed in order to take appropriate corrective action if higher satisfaction levels are desired.

- The 2000/01 IT purchases were consistent with IT plans and contributed toward greater standardization of the IT infrastructure. However, tendering practices should be strengthened to be able to consistently demonstrate that purchases are made with due regard for value for money.
- Many actions to promote appropriate security have been taken and we acknowledge the awareness and concern by the CS Department for adequate security. The College's increasing reliance on technology and the use of the Internet have significantly increased the security risks faced by the College. In light of this environment, we concluded that the College should take additional actions to minimize the risk of unauthorized access to its computer networks.

Our report contained 19 recommendations which are provided in full in the Detailed Findings and Recommendations section of the report. Some of the key recommendations are:

- that the College develop performance measures to assess progress towards achieving the IT Objective #6 (integrate Information Technology in the delivery, operation, and management of all College programs and services) set out in their strategic plan;
- that the CS Department update the asset management system and process changes in a more timely manner;
- that the College clearly assign responsibility for monitoring compliance with software license agreements and that a record of all software licensing agreements be maintained by the CS Department;
- that the College update its purchasing policies and procedures to better define and facilitate compliance with:
    - tendering guidelines,
    - the bid selection process, and
    - documentation requirements to support purchasing decisions;
- that the College conduct comprehensive security reviews on a periodic basis;
- that responsibility for College security, including IT security be assigned to an appropriate senior official or committee; and
- that the College better segregate its internal network from publicly accessible servers.

The College's responses to our recommendations have been included in the Detailed Findings and Recommendations section of the report and indicate that the College has already taken action to address a number of the recommendations.

2.0 Introduction

As the last chapter of our review of information technology (IT) in Manitoba's Community Colleges, we conducted a value-for-money audit of Red River College's (College) investment in IT. IT represents a significant annual investment of College resources, and is a key success factor in the College's achievement of its mission and goals. Similar audits have been completed and reports issued on Keewatin Community College and Assiniboine Community College.

IT is an important part of the success of any organization and Manitoba's community colleges play a vital role in providing state-of the-art training in the use of technology. IT is also used within a college environment to provide critical support to staff and students for administrative functions such as financial management, tracking student records, and helping staff work more effectively and efficiently by providing productively tools such as word processing and electronic spreadsheets.

IT has also revolutionized communications and with access to email and the Internet, College staff members can share leading-edge information with their contemporaries and students can conduct research, thereby enhancing the overall learning environment of the College. In addition, the use of IT for distance education offers the potential for a college to reach students that may not otherwise be able to take college courses without leaving their communities.

3.0 Audit Objective, Scope and Approach

The objective of our audit was to answer the following four questions:

1. Is the College making sufficient progress in achieving its information technology objective?
2. Are information technology systems and services adequately meeting the needs of users?
3. Are information technology purchases made with due regard for economy and effectiveness?
4. Is the College taking appropriate action to minimize the risk of unauthorized access to its computer networks?

Our examination was performed in accordance with value-for-money auditing standards recommended by the Canadian Institute of Chartered Accountants, and accordingly included such tests and other procedures as we considered necessary in the circumstances.

Audit procedures were performed during the period December 2001 through June 2002, and included examining available records and conducting interviews with College officials, administrative staff, and faculty.

In determining what appropriate and practical IT planning processes should be, we referred to standards for managing information technology issued by the Canadian

Institute of Chartered Accountants and the Information Systems Audit and Control Association.

With respect to Question 2, as part of our audit process, we conducted a staff satisfaction survey and completed IT user satisfaction survey questionnaires with over 400 College staff members (approximately 50% of full time instructors, administrators, and management staff). We also interviewed a small representative sample of 35 students to determine their level of satisfaction with College IT systems and IT support services.

A management consulting firm experienced in conducting security reviews assisted in our work on Question 4.

4.0 About the College

4.1 HISTORY AND ORGANIZATION OF THE COLLEGE

The College began offering training programs in 1938. In 1993, under The Colleges and Consequential Amendments Act, the College became a self-governing institution with a government appointed Board of Directors.

The College's purpose is set out in its mission statement:

> *"To build a prosperous and sustainable Manitoba through high quality applied education and research focused on advancing the economic, cultural, and social progress of people."*

In order to meet its mission, the College is committed to the following goals:

- providing a high quality learning experience to facilitate student success;
- increasing enrolments and participation rates in the college system by creating new responsive programs, improving current programs, and introducing innovative delivery methods to reduce barriers and facilitate access to education and training for Manitobans and meet the challenges of a changing economy;
- providing a safe, healthy workplace and a learning-centred environment that promotes peak performance and allows employees and students to participate and grow, respectful of each other and the diversity of the community and society;
- providing a vibrant learning environment through the development and enhancement of its infrastructure including the facilities, equipment, systems, and technology supporting the teaching and learning process;
- ensuring the financial strength of the organization through government funding, fundraising, and the development of business opportunities that advance the vision of the College; and
- supporting and enhancing the progress of Manitoba and its diverse, multi-cultural and Aboriginal heritage through public and community service arising from its learning focus and broad array of applied arts, science, and technology programs.

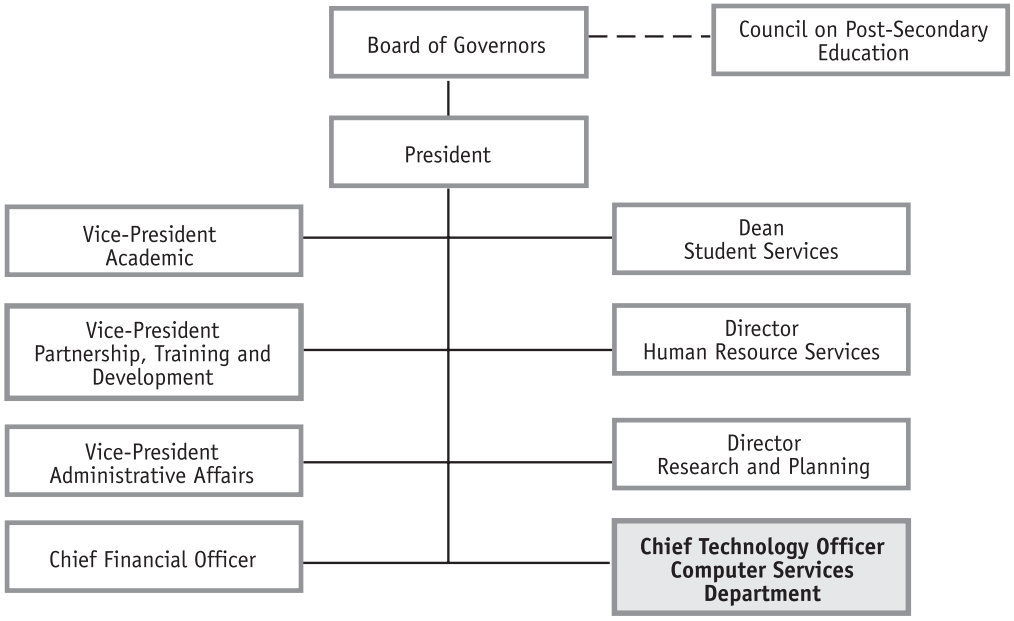
The College delivers over 110 diploma, certificate, and apprenticeship programs in the fields of applied arts and sciences, business, community services, developmental education, health, trades, and technology.

College programs are delivered in a number of locations in Winnipeg and Southern Manitoba. Winnipeg facilities include its main campus on Notre Dame Avenue, the Princess Street Campus, the Language Training Centre, and the Stevenson Aviation and Aerospace Training Centre. Regional campuses are located in Gimli, Winkler, Portage la Prairie, and Steinbach. As of June 30, 2002, 949 full-time and 217 part-time academic and administrative staff provide education services to approximately 7,800 full-time and 3,900 part-time students. In addition, 1,105 contract staff provide training to approximately 2,200 distance education students, 17,000 continuing education program participants, and 500 contract training program participants. The expenditure budget for 2001/02 was $81.0 million. Revenues included provincial grants of $47.0 million.

As reflected in Figure 1, the College is organized into 8 areas, each reporting to the President. For this value-for-money audit, we focused primarily on the Computer Services (CS) Department.

FIGURE 1

Red River College Organization Chart
(as of August 2001)



Source: Red River College

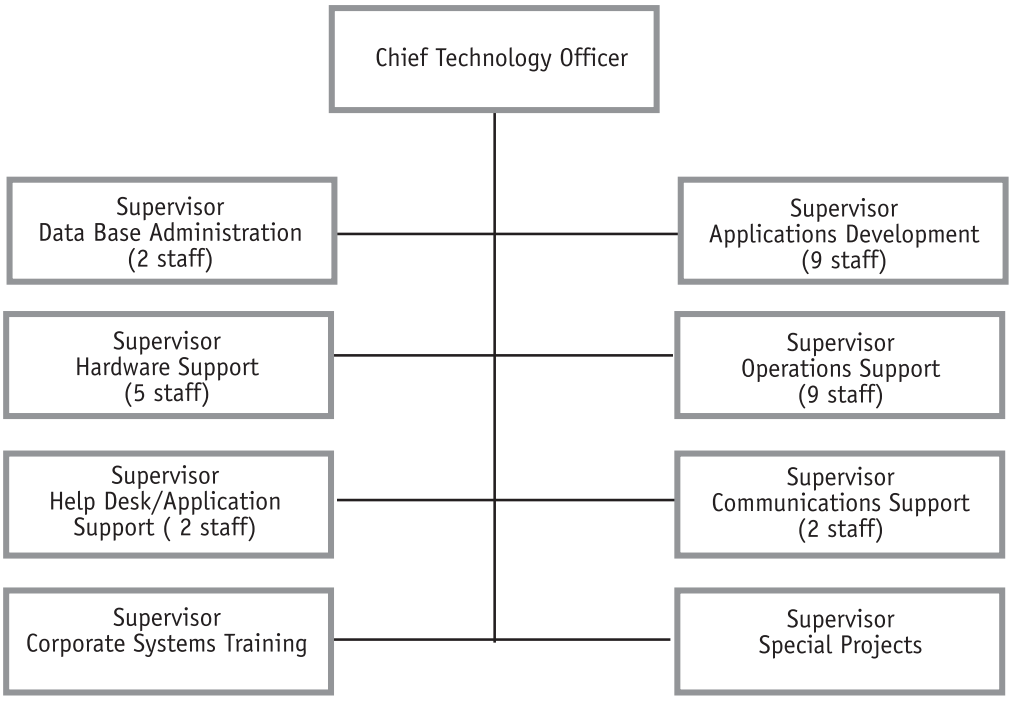
4.2 COMPUTER SERVICES DEPARTMENT

4.2.1 Organizational Structure

The Chief Technology Officer position was created in May 2001. At that time, the CS Department was delegated responsibility for college-wide information technology services. Previously, academic departments managed their technology needs with little involvement from the CS Department. Full implementation of these new responsibilities was a major undertaking and was implemented in stages. The Chief Technology Officer manages a complement of 37 staff positions as shown in Figure 2.

FIGURE 2

Computer Services Department
(as of March 2001)



Source: Red River College

While the CS Department is responsible for overall management of IT services, there are a number of academic departments where significant use of technology is integrated directly into academic programs. In these instances, academic departments continue to be responsible for course related IT services. Examples include "teardown" labs where students repair or build computers, and course specific help desk services to provide assistance to students in using specialized software as part of their program of studies.

The College has four widely dispersed regional campuses, a downtown training centre, and an aerospace training centre that place additional demands on the College's financial resources allocated to IT. Also the College has completed construction of the new Princess Street Campus that they refer to as a world class high-tech campus. The new campus will be home to more than 2,000 learners and 200 staff when it is fully operational.

4.2.2 Computer Services Department Mission

The CS Department's mission is *"to provide information technology services to support the operations of the college community in a timely and effective manner".*

4.2.3 Services Provided

The CS Department advises senior management on how IT can support the strategic direction of the College. Specific IT objectives are set out in the College's 5 Year Strategic and Operational Plans.

The CS Department provides services through the following eight functional areas:

Application Development

- Responsible for the implementation, integration, maintenance, upgrading, and on-going support of the College's corporate administrative computer systems, as well as software applications provided for specific localized areas within the College.

Database Administration

- Responsible for database design, integration, installation, maintenance, and upgrades, including web-based applications, purchased applications, and connectivity software.

Hardware Support

- Responsible for the installation and maintenance of all staff and laboratory computers and related equipment, as well as desktop management for all staff.

Operations Support

- Responsible for the maintenance of over 70 computer servers that run academic and administrative applications. Academic applications include student e-mail and desktop or laptop computer lab support. Administrative applications include intranet, staff e-mail, financial systems, and student information systems.

Communications Support

- Responsible for maintaining the College's computer network. This service includes internet access, fiber optic and cable systems, routers and switches, wireless networks, security and firewalls, remote access including dialup, virtual private networks and remote campus access, and network management.

Application Support

- Responsible for the operation of the College's Help Desk. Staff support is available in-person, by telephone, e-mail, and by using a staff web account.

Corporate Systems Training

- Responsible for providing courses on corporate web applications and major corporate systems including the Student Information System, Budget System, Outlook E-Mail, and Group Management.

Special Projects

- Provides support for leading edge technologies and new initiatives. Support services include assisting users with the design and implementation of information technologies and establishing or assisting cross-functional teams.

4.2.4 Statistical Information

Figure 3 shows a summary of IT expenditures and staffing information.

FIGURE 3

Summary of IT Expenditures and Staffing

	Actual			
	1998/99	1999/00	2000/01	2001/02
CS Department				
Number of staff	33	41	38	38
	$	$	$	$
Salaries and staff benefits	1,765,600	1,984,300	2,102,100	2,221,100
Hardware and software costs (Note 3)	427,700	420,100	327,300	364,300
Other	309,300	409,500	140,500	342,300
Total CS Department	**2,502,600**	**2,813,900**	**2,569,900**	**2,927,700**
Other Departments (Note 1)				
Student laptop computers (Note 2)	619,400	1,437,300	1,347,600	1,178,700
Hardware and software costs (Note 3)	1,319,500	916,300	1,069,500	529,900
Other computer related costs	8,800	13,700	23,800	12,700
Total IT expenditures other departments	**1,947,700**	**2,367,300**	**2,440,900**	**1,721,300**
Total IT related operating expenditures	**4,450,300**	**5,181,200**	**5,010,800**	**4,649,000**
IT Capital Expenditures				
Capital purchases	2,049,600	975,000	1,205,400	845,100
Capitalized leases	-	-	1,560,500	502,000
Total IT capital expenditures	**2,049,600**	**975,000**	**2,765,900**	**1,347,100**
Total IT operating and capital expenditures	**6,499,900**	**6,156,200**	**7,776,700**	**5,996,100**
Total College Expenditures (including capital expenditures)	**67,317,000**	**71,538,000**	**78,873,000**	**87,767,000**
Total IT costs as a percentage of total expenditures	**9.7%**	**8.6%**	**9.9%**	**6.8%**

Notes:
1. Other department figures do not include salaries that support IT activities (e.g., department help desks, educational assistants, etc.)
2. Student laptops are supported through a technology access fee charged to students.
3. Represents acquisition under $750, rentals, and repairs and maintenance.

Source: Red River College

4.3 SYSTEMS AND TECHNOLOGY

Student information is provided by a system that was developed in-house in 1996 and subsequently expanded and enhanced. The system includes the following components:

- student admissions and registration;
- account billings, payments, and sponsor information; and
- academic records.

Financial information is provided by a commercial software package that was installed in 1998. This system includes the following components:

- general ledger;
- accounts receivable; and
- accounts payable and purchasing.

Other information systems used by the College include:

- a library services system that provides students and staff with on-line access to the library's holdings and other library systems around the world;
- a point of sale system for the book store that records sales and provides information on merchandise inventory;
- an asset management system that records details of assets purchased;
- a payroll and personnel management system that prepares payrolls, records individual staff payroll information, and tracks sick leave and vacation;
- a system to log, maintain and report all user requests for service through the Help Desk; and
- personal productivity tools such as word processing, spreadsheets, and e-mail.

Distance education technology is utilized by the College to deliver selected courses over the Internet. Students can transmit many of their assignments to instructors electronically, and can also participate in chat rooms, class mail lists, and discussion boards. Through course content links, distance education students can also access the most current web sources for information and research.

The College maintains internal networks that are linked to the Internet. This structure provides the foundation for connecting all staff and students for all of the College's facilities.

The College also maintains an Internet web site that offers information about the College, extensive information for faculty and staff about various services, a staff directory, and a course and program search feature.

5.0 Systems and Technology Environmental Scan

The rapid rate of change regarding information technology has had a significant impact on the demands of information technology departments at colleges and universities across Canada. Several factors affecting the challenge faced by post secondary educational institutions regarding information technology are listed below:

- The transition from a mainframe based computing environment to the rapidly changing microcomputer based environment has significantly changed the nature and type of IT services provided and increased demand for direct service to users.
- Today, the majority of faculty, administrative staff, and students are users of information technology resources and services.
- Colleges and universities often purchase hardware and software on a piecemeal basis due to funding constraints. As a result, the systems are not standardized across the organization, and are therefore complex to support.
- Colleges and universities face challenges in staffing information technology positions. These challenges include fewer graduates in computer-related fields, lack of competitive salaries in the higher education environment, and increasing market demand for information technology skills.
- The Internet "revolution" is resulting in the proliferation of personal computing devices and people wanting self-serve access to information from anywhere at any time. The technological infrastructure of computers, networks, and software has to be kept up-to-date. Information technology staff need to learn new technologies and stay competent in current ones in order to successfully implement technological changes. Information technology departments may face demands to provide support almost twenty-four hours a day.
- Colleges and universities are delivering courses over networks, including the Internet and are competing in the delivery of these services. Being able to offer such services requires financial investments in computer hardware and software.
- The inclusion of up-to-date technology in academic programs is a critical success factor for many colleges and universities. In an effort to provide for an ongoing replacement and upgrade of technology, institutions are adopting innovative solutions such as "evergreen" policies that encourage the renewal of technology over fixed time frames.

6.0 Findings, Conclusions and Recommendations

6.1 IS THE COLLEGE MAKING SUFFICIENT PROGRESS IN ACHIEVING ITS INFORMATION TECHNOLOGY OBJECTIVE?

WHAT WE CONCLUDED

The College reported significant progress in completing most of the 2000/01 actions associated with the strategies flowing from the IT Objective #6 (integrate Information Technology in the delivery, operation, and management of all College programs and services) in the College's Strategic Plan (Figure 5). However, because the College had not developed sufficient performance measures for IT, we could not assess the degree to which the Objective was being met.

We reached this conclusion by examining criteria highlighted in the following findings sections.

WHAT WE FOUND

6.1.1 The Need to Update the CS Department's 5 Year Strategic Plan and Business Plan

Criteria

A multi-year IT strategic plan should be in place that links an IT department's annual operational plan to the strategic plan for the organization as a whole.

A multi-year IT strategic plan is an essential planning document because strategic goals and related objectives can be broad in nature and may require several years of effort to achieve. It also illustrates and communicates how IT initiatives contribute toward broader organizational strategies and goals. A multi-year IT strategic plan should detail the specific initiatives to be undertaken by an IT department to fulfill its objectives. As such, it provides vital direction for each year's operational plan. A multi-year IT strategic plan would include:

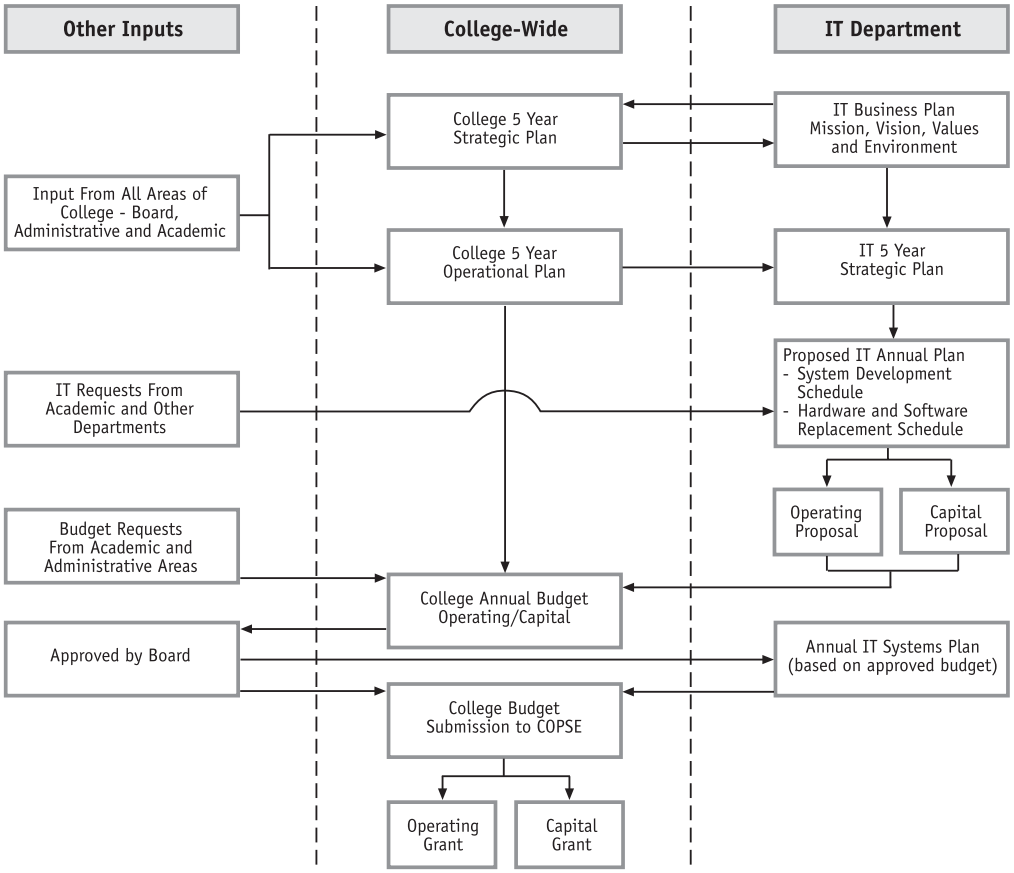
- *a multi-year infrastructure plan that would outline the proposed enhancements and modifications to the existing infrastructure to further the business objectives of an organization, as set out in the organization's strategic plan; and*
- *a multi-year acquisition plan that would outline how an IT department intends to replace computers and other components that become obsolete or wear out.*

A multi-year IT strategic plan would also describe the risks and potential lost opportunities associated with not proceeding with the various initiatives in the plan. This information is useful when evaluating competing funding requests because the merits of specific IT expenditures can be better evaluated against the relative merits of other proposed IT projects and of other organizational priorities.

The College has an annual College-wide strategic and operational planning process which results in the preparation of updated College-wide five-year strategic and operational plans. Figure 4 illustrates the process in place at the College.

FIGURE 4

Red River College
Planning and Budget Cycle



Source: Prepared by OAG in consultation with College management

The five-year plan articulated 12 college-wide objectives, including one IT objective (Objective #6), and identified various strategies and actions for each objective (Figure 5).

FIGURE 5

Red River College
College-Wide 5 Year Strategic Plan and Operational Plan Objectives

	Objectives	Number of Associated Strategies	Number of Associated Actions
1.	Deliver high quality programs and services that focus on the customer.	11	61
2.	Increase student success.	5	26
3.	Increase program offerings and ensure that programs and mix of programming responds to the diverse and changing needs of Manitobans and the workplace.	9	35
4.	Provide optimal accessibility to programs and services.	4	16
5.	Recognize, strengthen and reward the capabilities and contributions of employees, and support a respectful College environment.	3	13
6.	**Integrate information technology in the delivery, operation and management of all College programs and services.**	**6**	**17**
7.	Provide a safe and well maintained environment for working and learning.	5	23
8.	Continue the College's participation in global education.	4	12
9.	Strengthen collaboration and partnerships.	7	20
10.	Employ College resources effectively and efficiently and achieve financial strength and stability.	3	31
11.	Enhance the image and commitment of the College among staff, students and the external community.	5	23
12.	Enhance the learning centred focus and the innovative, and technologically advancing aspects of the College.	5	20
	Total Number of Strategies and Actions	**67**	**297**

Source: Red River College's 2002 - 2007 Strategic and Operational Plans

We noted that the College-wide plans outlined risks and opportunities including those specific to IT. Risks (challenges) for IT included:

- under funding for IT infrastructure;
- retaining currency in technology for academic purposes and administrative needs;
- IT security; and
- maintaining affordability of fees for student laptop computers.

Opportunities for IT included:

- increasing role of technology to manage 24/7 and e-commerce capability of learners; and
- growth in e-learning to support life-long learning using a variety of modes.

The CS Department prepared several plans as follows:

- **IT Business Plan** - set out the mission, vision, values of the CS Department and discussed the existing and planned IT environment;
- **5 Year IT Strategic Plan** - included the IT related objective in the College-wide 5 year strategic plan and outlined the hardware, software, staffing, and funds required for each of the five years to replace, enhance or expand the IT infrastructure at the College; and
- **Annual IT System Plan** – prepared for COPSE and sets out risks and opportunities and provides details regarding initiatives and tasks to be undertaken by IT during the year.

We are concerned that the CS Department's IT Business Plan and 5 Year IT Strategic Plan have not been updated for several years. The CS Department's IT Business Plan was last updated in September 1997 and that the CS Department's 5 Year Strategic Plan for the period 1999 to 2004 was last updated in November 1998.

Because these plans had not been updated, they did not reflect several recent significant IT related initiatives including:

- the new College-wide strategy regarding e-commerce, e-learning, and e-business;
- the 2001/02 "evergreen" plans for hardware replacement over 3 years;
- the addition of the Princess Street Campus;
- Stevenson Aviation Centre IT requirements;
- expanded role of the Chief Technology Officer regarding IT for the entire College; and
- an updated discussion of risks and challenges.

In addition, the Annual IT Systems Plan prepared for COPSE was not explicitly linked to the objectives and related strategies and initiatives in the CS Department's 5 Year IT Strategic Plan.

As a result, these documents were not effective in communicating how the planned priorities of the CS Department contributed towards accomplishing the College-wide IT objective the CS Department was mandated to pursue.

R1 We recommend that the CS Department update its strategic and business plans on an annual basis and ensure that these plans are clearly linked to the IT objective in the College's 5 Year Strategic Plan and the Annual IT Systems Plan.

COMMENTS OF OFFICIALS

The CS Department develops each year's Systems Plan based on its participation in both the strategic planning and budget processes as well as working with various constituents and committees throughout the College. The System Plan functions as both the strategic and business plans for the CD Department.

In addition, as a part of the five-year strategic planning process, the CS Department develops critical IT objectives, strategies and actions as well as provides a status on previous activities. As part of the budget process, the CS Department is made aware of new initiatives requiring computer resources. As members of committees such as the Teaching and Learning Technology Roundtable, the CS Department helps develop a strategy for the academic environment.

6.1.2 The Need to Include Sufficient Detail in the Annual IT Systems Plan

Criteria

An annual IT operational plan should be in place that includes the specific tasks to be accomplished, the resources required to complete the tasks, and the timelines for completion.

The 2001/02 Annual IT Systems Plan included nineteen major initiatives along with a description of each of these planned initiatives. However, we noted that the plan did not include the resources needed and timelines for completion of the initiatives. We observed that this information was included in other internal documents, as follows:

- 1999 to 2004 CS Department's 5 Year IT Strategic Plan provided estimates of funding requirements and type of resources required for each action;
- 2001/02 annual CS Department system development schedule provided details of major system enhancements and developments together with resources assigned to each main element; and
- 2001/02 annual CS Department hardware and software replacement schedules provided details of various components to be replaced.

Summarizing key aspects of the above noted information in the Annual Systems Plan would provide senior College management with better information on IT initiatives and their impact on the College resources.

R2 We recommend that the CS Department include key scheduling and resource decisions for significant initiatives in the CS Department's Annual IT Systems Plan.

COMMENTS OF OFFICIALS

Management agrees with audit recommendation R2. The CS Department will include key scheduling and resources for significant initiatives in its annual Systems Plan.

6.1.3 The College Reported Significant Progress in Accomplishing Planned Actions.

Criteria

Progress in achieving strategic objectives, including operational plan initiatives, should be monitored.

College-wide progress in relation to its planned actions is reported annually in a public report titled "*Report of Strategic Plan Achievements at Red River College*".

In their report for 2001, for the 17 detailed actions associated with the Strategic Objective #6 that the College integrate information technology in the delivery, operation, and management of all College programs and services, the College reported:

- significant progress for 14 actions;
- moderate progress for 2 actions; and
- preliminary stages for 1 action.

The detailed status of each of the actions as at December 31, 2001 is set out in Appendix A.

Management indicated that the status of the actions detailed in the report were accurately described.

6.1.4 The Need to Develop Performance Measures

Criteria

Performance measures should be in place to help assess progress made in achieving strategic objectives.

Clearly defined performance measures and targets are critical to ensure the effective management of IT resources and the adequacy and appropriateness of actions planned and taken to meet management's expectations.

The College's strategic and operational plans set out three high level performance indicators for the College's main IT Strategic Objective #6 of integrating information technology in the delivery, operations, and management of all College programs and services. These performance indicators were centered on stakeholder satisfaction with:

- the degree of technology training incorporated within academic programs;
- the degree to which technology is integrated within the administrative operations of the College; and
- the ability to access necessary information and communication tools.

The CS Department's 5 year IT Strategic Plan identified 17 specific actions (Appendix A) that address the College's main IT strategic objective. However, the College has not developed performance measures to assist management in determining how or to what extent these actions will provide the College with the results they expect. For example, to help assess whether the College has made satisfactory progress in establishing a primary, reliable College communication system, performance measures would need to be developed for the actions required to achieve this target. These could include measuring electronic communications to determine the increase in usage over other forms of communication, or the acceptance and use of electronic services such as course outline preparations, registration, student achievement, and other student services.

The College is in the process of collecting information on IT performance indicators in preparation for developing specific performance indicators for IT services at the College. However, because performance measures and targets had not been developed at the time of our audit, the College was not in a position to determine how well the CS Department was meeting the performance expectations contemplated by management when the strategic plan was prepared.

R3 We recommend that the College develop performance measures to assess progress towards achieving the IT Objective #6 (integrate Information Technology in the delivery, operation, and management of all College programs and services) set out in their strategic plan.

COMMENTS OF OFFICIALS

Management agrees with audit recommendation R3. The College will develop performance measures as recommended.

6.2 ARE INFORMATION TECHNOLOGY SYSTEMS AND SERVICES ADEQUATELY MEETING THE NEEDS OF USERS?

WHAT WE CONCLUDED

The majority of users surveyed or interviewed indicated that they were generally satisfied with IT systems and services. Opportunities still exist for the College to regularly gauge whether user needs are being adequately addressed in order to take appropriate corrective action if higher satisfaction levels are desired.

We reached this conclusion by examining the criteria highlighted in the following findings sections.

WHAT WE FOUND

6.2.1 Most Users Indicated That They Were Satisfied With the Nature and Quality of Information and Reports

Criteria

Users should be satisfied with the nature and quality of information generated by the information system.

Organizations should periodically determine the level of user satisfaction with IT systems and services to ensure that they are receiving value for their investment in information technology.

By measuring user satisfaction, organizations can better determine if user needs are being met and can identify opportunities to improve services. In addition, by measuring user satisfaction at regular intervals, an organization can determine whether its improvements in IT services, over time, are resulting in the desired effects.

In our view, one of the best measures for the adequacy of information generated is the level of user satisfaction. As such, we gained insight into this area by surveying staff on their satisfaction with information received.

Survey responses indicated that 22% of College staff were very satisfied and 62% were satisfied (total of 84%) with the information and reports generated by College information systems. In addition, 65% of respondents indicated that information and reports had improved over the last two years. No respondents indicated that information had deteriorated.

We encourage the College to continue its ongoing efforts to improve generated information and reports from College systems.

6.2.2 The Need to Define and Monitor Service Levels

Criteria

Service levels should be defined and monitored.

The level of support that an organization can reasonably expect from an information technology support function is largely determined by the level and quality of human resources made available and the quality of hardware and software. With these factors in mind, an organization should define the service levels expected and provide resources accordingly. Service levels can be defined in a number of ways including system response times, security provided, system functionality, and helpdesk service response times. Expected service levels should be communicated to users and should serve as performance criteria to measure the quantity and quality of service levels achieved. Appropriate actions should be taken to address performance shortfalls.

While the College had defined and communicated the nature of its IT services, expected service levels were not defined. Understanding service levels achieved, in relation to expected levels, would help the College determine the adequacy of both its technological capacity and the level of human resources devoted to the CS Department.

A help desk was in place at the College and requests for assistance were recorded in a central log. Guidelines were established for prioritizing and for assigning problems to the most appropriate person. In addition, we were informed that requests for assistance are monitored to ensure that they are appropriately resolved.

Because expected service levels were not defined or tracked by the College, we could not conduct a direct review and assessment of the adequacy of service levels provided by the CS Department. Nonetheless, 73% of respondents to our survey indicated that they were generally satisfied with the CS Department's current service delivery, and 44% agreed that services had improved over the last two years.

In addition, our user satisfaction survey indicated a fairly high level of satisfaction with the assistance provided to staff by the help desk (73%), but also showed that 11% of respondents were dissatisfied with the assistance provided.

We noted that students reported a lower level of overall satisfaction with support services with only 52% satisfied and 19% unsatisfied (29% were neutral). However, 70% of students reported that they did receive the help requested, and 74% reported that they were satisfied with the response time by the CS Department.

R4 We recommend that management define the expected service levels to be provided by the CS Department, communicate these service levels to users, and then monitor their achievement of these service levels through the use of outcome oriented performance measures.

COMMENTS OF OFFICIALS

Management agrees with audit recommendation R4 and will define, communicate, and monitor service levels for the CS Department.

6.2.3 A System is in Place to Manage Requested Changes to Systems or Reports

Criteria

User requests for changes to systems or reports should be effectively managed.

Changes to an organization's information systems are inevitable as management responds to the demands of a changing environment. Organizations must carefully manage this change process in order to ensure its information systems continue to address the needs of its users.

Organizations should log requests for changes to a system, assess these requests for needed actions, prioritize the requests, and monitor progress made in responding to the change requests. Once a solution has been developed, users should formally test and approve the changes to the system. This helps to ensure that the problem has been appropriately addressed. Dealing with change requests in a timely manner minimizes the likelihood of disruptions to users over a prolonged period of time caused by system errors or systems that do not address important user needs.

We limited our work within this area to obtaining an understanding of the process followed by staff and to a limited examination of logs and system changes. We were advised that all requests for changes were recorded by CS Department staff in an automated system called "Case Log". Key information recorded in the log included:

- name of the requestor;
- date of the request;
- reason for and description of the change; and
- requested date for implementation of the change.

Requests were assessed in terms of the resources required, estimated costs, priority of the change, risks associated with the change, and any fallback procedures required. Request priority was determined by a committee of users, and for major changes, the priorities were reviewed and approved by the President's Council.

Once approved, systems change requests were assigned to a CS Department staff member and scheduled. CS Department staff members advised that they worked closely with users to ensure the system changes met their needs. Changes are tested and approved in writing by users before being implemented. System change documentation is prepared and retained.

In addition to reviewing the system in place for managing change requests, we also surveyed staff on their satisfaction with the systems they use. Survey responses indicated that 35% of College staff were very satisfied, and 49% were satisfied (total of 84%) with College systems. In addition, 75% of respondents indicated that College systems had improved over the last two years; and only 2% of respondents indicated that systems had deteriorated.

We noted that students interviewed also reported a high level of satisfaction with College systems with 77 % either satisfied or very satisfied; only 9% were unsatisfied.

6.2.4 Formal Standards and Procedures for Supporting Information Technology are in Place

Criteria

Formal standards and procedures for supporting information technology should be in place.

Such standards and procedures are important because they help prevent, or minimize, the impact of disruptions in computer services. The risk of disruption is reduced because:

- *computer hardware and software are more likely to be installed, configured, and operated in a consistent and appropriate manner; and*
- *other support functions, such as recovering from computer system "crashes", backing up data, and maintaining hardware are more likely to be performed in a timely and orderly fashion.*

The CS Department had developed formal standards for installing, maintaining, and operating the College's technological infrastructure. These standards include naming standards for each element, installation procedures, and testing procedures. The database administration section of the CS Department maintains daily checklists to document compliance with these standards and procedures. The CS Department also maintains a database administration manual that documents the detailed security procedures to be followed for each application.

6.2.5 The Need to Update IT Asset Management Records

Criteria

Complete asset management records should be maintained to account for information technology components.

Maintaining complete records of information technology assets is a necessary component of an organization's efforts to manage and safeguard those assets. Asset management records should identify information technology components and associated information, such as physical location, serial and model numbers, configuration details, and software licenses. These records are an important control feature because they help an organization account for all information technology components, and are essential in conducting periodic verifications of physical existence. In addition, when configuration details are noted, these records facilitate the efficient management of changes to technological infrastructure components.

A new IT asset management system was implemented in the summer of 2001. This system enables the recording of appropriately detailed asset management information such as component part specifications, physical location, serial and model numbers, and other configuration information. However, we found that the information in the IT asset management system was not accurate nor up to date. Our testing results include:

- from our 2000/01 sample of 488 purchases, 160 had not yet been recorded in the IT asset management system;
- from our sample of 191 items that we physically examined, 39 items were not recorded in the IT asset management system; and
- from our sample of 152 items recorded in the IT asset management system, 44 items were physically observed in rooms that were different than the location recorded in the system.

R5 We recommend that the CS Department update the asset management system and process changes in a more timely manner.

COMMENTS OF OFFICIALS

At the time of the audit, the CS Department was in the process of implementing and converting data for the new IT asset management system. To help maintain accurate records, the CS Department has implemented an inventory tracking software package in conjunction with upgrades to this system.

6.2.6 The Need to Monitor Academic Software License Agreements Centrally

Criteria

Compliance with the provisions of software license agreements should be monitored.

Software license agreements set out the parameters for use of the software and often contain restrictive provisions such as limiting the number of users. Organizations should take reasonable steps to monitor compliance with the acceptable use provisions of software license agreements.

We reviewed four of the College's main corporate software license agreements and noted that the CS Department monitored usage to ensure compliance to the requirements of the license agreement.

We also reviewed three academic software license agreements. We noted that two of the academic departments monitored for compliance with the license agreements. However, for the other academic software, neither the academic department, nor the CS Department monitored for compliance to the software agreement. We also noted that the College could not locate the software licenses for either of the two student laptop computer leasing agreements. College policies are silent regarding responsibility for this important function.

Failure to appropriately monitor compliance with software license agreements increases the risk that the College will unknowingly violate software licenses.

R6 We recommend that the College clearly assign responsibility for monitoring compliance with software license agreements and that a record of all software licensing agreements be maintained by the CS Department.

COMMENTS OF OFFICIALS

Effective December 3, 2002, the College approved a new best practice guideline entitled "Development and Administration of Agreements". As recommended by the guideline, a central registry of software license agreements is now maintained by the College's Corporate Legal Services department. A record is also maintained by the CS Department. Compliance is the responsibility of the user department.

6.2.7 The Need to Assess the Availability, Quality, and Timeliness of IT Training Opportunities

Criteria

Users should have access to IT training opportunities.

In order for an organization to maximize the value it receives from investing in information technology, an organization must ensure that users receive appropriate and timely training on the systems and automated productivity tools available to them.

We were advised that courses are provided to new system users. The College also provides training on an ongoing basis to staff, and has established a dedicated training room for this purpose.

The College has indicated its commitment to staff development in all areas including information technology. We understand that the College offers training and staff development to employees in a number of different forms. In addition to specific training opportunities delivered by the CS Department itself, a central staff development office provides support for identifying external training, develops internal training and maintains a database of training courses that employees attend. College employees are also eligible to attend relevant Continuing Education opportunities.

Notwithstanding the College's efforts to meet staff training needs in the area of information technology, our staff survey indicates that staff expectations have not been adequately met.

While an organization may not be able to satisfy the training needs of all staff, many respondents to our survey reported that IT training could be improved:

- While 51% of respondents agreed with the statement, *"I am provided with training on how to use systems applicable to my job"*, 26% reported that this was true only some of the time, and 23% (more than one in five employees) did not agree with this statement. When asked, *"Is there any specific computer training that would help you do your job better?"*, the most requested training was for productivity software for word processing, spreadsheet preparation, presentation preparation, and database software (31%). Respondents also requested more hands on training and workshops in general (14%).
- While 49% of respondents agreed that the training they received provided them with the necessary knowledge they needed, 26% reported that this was true only some of the time, and 25% (one in four employees) did not agree with this statement.
- While 50% of respondents agreed that the training was provided in a timely fashion, 26% reported that this was true only some of the time, and 24% (almost one in four) did not agree with this statement.

In addition, we noted that only 49% of respondents to our survey indicated that user manuals, instructions, and on-line help were available to them. Only 45% of respondents found user manuals, instructions, and on-line help clear and easy to understand.

R7 We recommend that the College conduct a more detailed assessment of the IT training needs of staff in order to ensure that the appropriate level and type of training is available to users.

COMMENTS OF OFFICIALS

The College has an ongoing commitment to staff development. Although current resources levels may not permit a detailed assessment of IT training needs, College staff are kept fully informed of all training opportunities available to them and are encouraged to notify the staff development office and/or the CS Department concerning their training needs.

6.3 ARE INFORMATION TECHNOLOGY PURCHASES MADE WITH DUE REGARD FOR ECONOMY AND EFFECTIVENESS?

WHAT WE CONCLUDED

The 2000/01 IT purchases were consistent with IT plans and contributed toward greater standardization of the IT infrastructure. However, tendering practices should be strengthened to be able to consistently demonstrate that purchases are made with due regard for value for money.

We reached this conclusion by examining criteria highlighted in the following findings sections.

WHAT WE FOUND

6.3.1 The Need to Strengthen the Tendering Process

Criteria

Purchases should be based on an appropriately conducted tendering process.

Tendering purchases helps to ensure that the lowest price is paid for the quality and quantity of product required. Essential elements of an effective tendering process include:

- *documented policies and procedures;*
- *clearly defined specifications for the equipment or service to be provided;*
- *solicitation of quotes from several suppliers to ensure competitive bidding on the tender;*
- *clearly defined selection criteria that include not only the price, but also other critical factors such as quality, delivery time, and product warranties; and*
- *documented analysis of quotes received to support the selection decision.*

We reviewed the College's purchasing policies and procedures. The Board policy, approved in 1998, requires that the College's purchasing systems "provide for comparisons for price, quality, service support, and long term effectiveness for all purchases over $2,500". We found that the College's purchasing procedures have not been revised since 1994, and do not adequately reflect these expectations.

As a result, we encountered the following issues in our review of IT purchases in 2000/01:

- Significant IT purchases were not tendered.
- Leasing decisions and selection of leasing agents were not adequately documented.
- All IT purchases were not reviewed and approved by the CS Department.
- IT purchases over $100,000 were not subject to a national tendering process.

Significant IT Purchases Should Be Tendered

As detailed in Figure 6, we sampled 39 IT acquisitions in 2000/01 totaling $2,355,000 from a total population of $3,576,000 for IT acquisitions. Purchases in the sample ranged from a low of $ 6,000 to a high of $610,000. We found that:

- only six purchases were tendered or competitive quotes received ($232,000); and
- documented explanations for not tendering were not prepared for the other 33 purchases.

The following table summarizes the results of our audit regarding non-tendered purchases:

FIGURE 6

Red River College
Summary of IT Purchases/Leases Reviewed

Value Range	Number of Transactions Reviewed	Total Value $	Initiating Department		Tender or Quotes Requested	No Tender or Quote
			CS Dep't.	Other		
< $ 10,000	1	6,063	-	1	-	1
$ 10,001 - 25,000	17	281,131	3	14	-	17
$ 25,001 - 50,000	10	369,857	4	6	4	6
$ 50,001 - 100,000	6	414,688	5	1	2	4
> $ 100,000	5	1,283,858	4	1	-	5
Total	**39**	**$2,355,597**	**16**	**23**	**6**	**33**

The College provided verbal explanations supporting their purchasing decisions that included sole source suppliers, preferential educational pricing, the need to maintain compatibility of equipment, and "benchmarking" costs against previous purchases.

However, we found no documentation to support the rationale for these purchasing decisions.

R8 We recommend that the College update its purchasing policies and procedures to better define and facilitate compliance with:

- **tendering guidelines;**
- **the bid selection process; and**
- **documentation requirements to support purchasing decisions.**

COMMENTS OF OFFICIALS

Management fully endorses audit recommendation R8. The President's Council approved a revised purchasing policy effective December 17, 2002. The policy formalized the College's previously established purchasing practices. It appears that certain purchases were made outside of these established practices. In some cases IT purchases were made to ensure equipment and system compatibility and to ensure Course Program deliverables. Management will review each of the purchasing anomalies identified within the Audit with a view to ensure processing compliance.

Competitive Bids For Leasing Arrangements Should Be Obtained

For the 2000/01 student laptop computer and network server leases, we noted that requests for quotes did not require that proposals include a lease financing option and only solicited quotes based on outright purchase of the equipment. Suppliers were selected on the basis of a purchase arrangement. The decision to lease occurred after the vendor selection.

We are concerned that all suppliers who bid on an outright purchase basis were not provided with the opportunity to also submit quotes on a lease basis. As such, the College cannot be assured that its selection of the leasing agent was based on the best proposal.

College officials advised that at least two quotes had been obtained for each of the leasing arrangements, but documentation of this process was not available.

Without appropriate documentation to support its leasing decisions, the College cannot demonstrate that the best value was obtained.

R9 We recommend that the College's major IT acquisition RFP's also include a request for quotes for lease options.

COMMENTS OF OFFICIALS

Management supports audit recommendation R9 and will ensure that RFPs include request for quotes for lease options and that all requests are documented.

The CS Department Should Approve All IT Purchases

For the sample of 39 IT purchases reviewed in 2000/01 (Figure 6), we noted that 16 of the purchase orders were initiated by the CS Department and approved by the Chief Technology Officer. However, there was no evidence of any CS Department review and approval of the other 23 purchase orders that were initiated by other departments.

Lack of review and approval of all IT purchases by the CS Department could result in the purchase of hardware or software that may not be consistent with the CS Department's plans for the College as a whole. Inappropriate hardware or software could have negative effects on the College's networks and could cause the network to slow down, cause crashes, or impair network security.

While we were informed that none of the 23 above noted purchases negatively impacted on the College's networks or security, the Chief Technology Officer advised us of other IT purchases made by other departments in previous years that either impaired the network security or caused the network to slow down or crash. These purchases included non-standard screen savers, color printers, and modems.

R10 We recommend that the College's purchasing policy require that the CS Department review and approve all IT purchases.

COMMENTS OF OFFICIALS

It has been a longstanding practice that the CS Department review and approve all IT purchases. Management agrees with audit recommendation R10. This recommendation has been formally included in the revised purchasing policy effective December 17, 2002.

Tenders For Purchases Greater Than $100,000 Should Be Subject To A National Tendering Process

The Agreement on Internal Trade (AIT), which came into effect in July 1995, provides a "*framework to ensure equal access to procurement for all Canadian suppliers*". The AIT required that, effective July 1, 1999, all purchases of goods and services over $100,000 and construction valued over $250,000 be subject to a national tendering process. In Manitoba colleges and universities were instructed to comply with the AIT, and to facilitate compliance, they were advised that they could post and distribute tenders on the MERX system, an electronic tendering bulletin board at no charge.

We found that the five 2000/01 IT equipment purchases (Figure 6) that exceeded $100,000 in value were not subject to a national tendering process.

R11 We recommend that the College's purchasing policy require that tenders for purchases greater than $100,000 be subject to a national tendering process.

COMMENTS OF OFFICIALS

Management supports audit recommendation R11. Our current purchasing policy requires that tenders for purchases greater than $100,000 be subject to a national tendering process. This practice has

been in place since 1999. Management will undertake a review of those purchases identified in the Audit to ensure ongoing compliance.

6.3.2 The Technological Infrastructure is Standardized to an Appropriate Extent

Criteria

The technological infrastructure (computers including the operating systems, peripheral components, and common application software) should be standardized to an appropriate extent.

An additional aspect in ensuring IT acquisitions are effective involves having an appropriate planning process to guide acquisition activities. In our view, effective acquisitions are those which support the business and academic objectives of the College, promote the efficient functioning of the IT infrastructure and support functions, and meet user needs.

The main elements of the IT infrastructure at the College were standardized to an appropriate extent. In addition, the need for standardization is embedded in the 2001/02 Annual IT Systems Plan which stated that standardization and integration of all corporate systems using common application software and hardware components was the underlying principle of the initiatives in the CS Department.

Computers

At the time of our audit, there were approximately 1,600 computers in use at the College. We noted that the College purchased 319 computers in 2000/01 and 573 computers in 2001/02. The 2000/01 purchases were in keeping with the number of planned replacements in the CS Department's 2000/01 replacement schedule. In 2001/02, the CS Department began implementing its three year replacement policy called "evergreen". The CS Department considers a 3 year life cycle to be an appropriate target for replacement of its computers. The 2001/02 purchases of 573 computers were in keeping with the new "evergreen" replacement policy.

Computer purchasing decisions by the CS Department were guided by minimum requirements for computers and other IT equipment that were developed by the CS Department and updated annually. We determined that the 2000/01 and 2001/02 computer purchases met those specifications and were compatible with the existing infrastructure. In addition, according to IT asset management records, the main hardware components connected to the network, with the exception of approximately 300 computers, met or exceeded the 2000/01 minimum standards. We noted that most of these computers were scheduled for replacement in 2002/03 under the new "evergreen" policy.

Software

We were told that the CS Department continually monitored available software upgrades and enhancements and made changes to software as circumstances allowed. During our audit, we noted that the CS Department was in the process of upgrading the College's operating systems and productivity software (spreadsheet, word processing, etc.) to a more current version of the software.

6.4 IS THE COLLEGE TAKING APPROPRIATE ACTION TO MINIMIZE THE RISK OF UNAUTHORIZED ACCESS TO ITS COMPUTER NETWORKS?

WHAT WE CONCLUDED

We observed that many actions to promote appropriate security have been taken and acknowledge the awareness and concern by the CS Department for adequate security. The College's increasing reliance on technology and the use of the Internet have significantly increased the security risks faced by the College. In light of this environment, we concluded that the College should take additional actions to minimize the risk of unauthorized access to its computer networks.

We reached this conclusion by examining the criteria highlighted in the following findings sections.

WHAT WE FOUND

6.4.1 The Need for Enhanced Administrative Support

> ***Criteria***
>
> *Security measures should include appropriate administrative support.*

Securing information and systems is a difficult task in a dynamic environment that is impacted by the actions of all users. Over and above the specific measures to prevent or detect security breaches, are the administrative elements that promote and contribute towards a security conscious environment.

We identified the following opportunities to strengthen administrative support:

- Comprehensive security reviews should be conducted.
- Responsibility for College wide security should be assigned.
- Updated and more comprehensive disaster recovery plans should be in place.
- A security awareness framework should be in place.

Comprehensive Security Reviews Should Be Conducted

Criteria

An essential element in safeguarding an organization's investment in information and related technology is managing the risks associated with appropriate physical and electronic access to information, hardware, and software. As a result, an organization should periodically assess the effectiveness of security controls in place. To be practical and cost effective, the rigor of the assessments should be commensurate with the sensitivity of the information, and the value of the hardware and software. Deficiencies and concerns arising from the assessments should be resolved on a timely basis to ensure controls are adequate to safeguard hardware from theft or damage, and software and information against damage, loss, unauthorized use, disclosure, and modification.

In our discussions with CS Department staff, we found a high degree of security awareness. The CS Department has been able to provide a reasonably sound level of security.

The CS Department conducts periodic security tests that include penetration testing of its networks. The test results are documented and followed up. However, the test procedures in themselves do not constitute a comprehensive security review. Given the large, sophisticated and decentralized networks like those managed by the College, we believe that periodic comprehensive security reviews are essential.

R12 We recommend that the College conduct comprehensive security reviews on a periodic basis.

COMMENTS OF OFFICIALS

Security is a major concern of the College. Currently the CS Department has one member certified as a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM), one with CISSP certification, and two in the process of certification for CISM. Since the period covered by the audit, the CS Department has added a Supervisor of Security and Special Projects responsible for all aspects of computer security. The CS Department will conduct comprehensive security reviews on a periodic basis and will incorporate external resources as required.

Overall Responsibility For College Security Should Be Assigned

Criteria

An organization should appoint a single, high level, individual/committee (other than technical line management) to take overall responsibility for all security matters including security of information technology and physical security of the buildings and other property.

The College has not assigned overall security responsibility to a single security authority. The absence of a single security authority can lead to shortfalls in threat and risk assessment, in security planning, and in response to security incidents and disasters.

The Chief Technology Officer has assumed the responsibility for duties normally attributed to an IT security officer and has assigned specific IT security tasks to different CS Department staff. However, these tasks are often performed on an "as required and when available" mode.

The lack of an overall integrated and coordinated approach to security management, including clearly assigning IT security responsibilities, likely contributed to the issues discussed in this section of the report.

R13 We recommend that responsibility for College security, including IT security be assigned to an appropriate senior official or committee.

COMMENTS OF OFFICIALS

Management agrees with this recommendation. Although Campus security and IT security currently report through different senior management officials, all security is ultimately the responsibility of the President's Council, the College's senior policy and operations committee.

Disaster Recovery And Business Resumption Plans Should Be Updated

Criteria

Prudent business practices include the preparation of a disaster recovery plan.

We reviewed the College's Disaster Recovery Plan and Emergency Procedures. While we were encouraged that such a plan existed, we noted that very few threats and scenarios were contemplated in the plan. We further noted that a copy of the Disaster Recovery Plan was not kept off site.

R14 We recommend that the Disaster Recovery Plan and Emergency Procedures be updated based on the results of a comprehensive threat and risk assessment and that a copy of the plan be stored off campus.

COMMENTS OF OFFICIALS

The disaster recovery plan was developed to handle any disruption in computer services. As time and resources permit, different scenarios will be developed and added to the plan. The plan will be stored off site.

A Security Awareness Framework Should Be In Place

Criteria

Security is a subject to which most people need to be sensitized, before they can appreciate the ramifications. A security awareness framework that includes security related policy and procedures, guidelines, strategies, and training material would help ensure that users do not unknowingly jeopardize the organization's security measures. A proactive approach is superior to a reactive one.

A comprehensive security awareness framework (policy and procedures, guidelines, strategies, and training material) does not currently exist.

Over the past decade, the College developed a number of security oriented policies and procedures. However, these polices have not been updated, nor has a comprehensive security policy and procedures manual been developed. Security policies and associated procedures should include personnel security; physical security; electronic security (computers, networks, electronic storage means); printouts; access control, both physical and electronic; telecommunications; disposal of IT equipment and data storage media; and incident reporting.

At the start of each academic year, all students receive security and acceptable use briefings by members of the academic staff. However, such briefings are not given to College staff.

R15 We recommend that the College develop a security awareness framework.

COMMENTS OF OFFICIALS

The CS Department has assigned computer security to the Supervisor of Security and Special Projects and awareness to the Supervisor of Corporate Training. Various pieces of the awareness framework exist and will be integrated into an overall security framework.

6.4.2 The Need to Improve Physical Security in Certain Locations.

Criteria

Physical security controls to safeguard IT assets should be in place.

The College has taken many appropriate steps to protect its investment in hardware, software, and information from physical threats such as fire, theft, and vandalism. We noted that:

- physical access to the main CS Department server rooms was well controlled and limited to authorized personnel; and
- fire extinguishers were checked on a regular basis.

However, we inspected several program area server rooms and found that they were not appropriately constructed to ensure adequate physical security. In some cases, they did not have automatic water sprinklers, fire and/or smoke alarms, appropriately placed fire extinguishers, and were sometimes used for storage. In one location, we found poor door locks and that access was inadequately controlled.

R16 We recommend that the College ensure all server rooms are appropriately protected from physical threats.

COMMENTS OF OFFICIALS

Management agrees with audit recommendation R16. Security Services, the Facilities Department, and the CS Department will conduct a comprehensive audit to identify potential security breaches with respect to all server rooms. Funding for security quite often competes against a long list of deferred maintenance items, specifically those relating to workplace safety and health.

6.4.3 Electronic Access Controls are Generally Adequate

Criteria

Controls to limit electronic access to information and systems should be in place.

A secure organization must ensure that systems and data are protected from unauthorized electronic access. This is required to protect systems and data from alternation, loss and unauthorized use. Electronic access can occur from network connections, dial up connections and web site connections.

The CS Department controlled access to network software and the Internet on a continuous basis with software, and had appropriate controls over the use of passwords.

The College did not encrypt system data such as personal and health information transmitted between College locations.

While the College had activated the audit or event log preparation features of various software programs, it was not monitoring these logs to identify inappropriate access attempts or internet usage. Information on access attempts would help the College identify and rectify key vulnerabilities. Likewise, by monitoring Internet use, CS Department staff could determine if College staff or students were accessing web sites deemed inappropriate by management and take appropriate action to "block" access to these sites or remove a user's access to the Internet.

R17 We recommend that the College encrypt sensitive information when transmitting between locations.

COMMENTS OF OFFICIALS

In the past, communication to external sites was over direct communication lines without the need for encryption. Over the last three years, the CS Department has undertaken to upgrade communication lines between sites to improve the speed and reduce the cost. Various methods have been used to protect the sensitive nature of this data. It is the goal of the CS Department to provide secure transmission of data from any point to any other point.

R18 We recommend that the College monitor activity logs to identify inappropriate network access attempts and internet usage. The College should also consider using logon banners to inform system users of monitoring policies and practices.

COMMENTS OF OFFICIALS

As space on the logon screen is limited, the College uses the logon screen to inform users that the CS Department monitors communications and to refer to the College's Acceptable Use of Computer Facilities Policy for further information. All corporate users must sign a document indicating that they have read this policy before they are assigned network access and accounts.

The CS Department also uses various software products to identify, prevent, and track misuse of computer systems and networks. The CS Department continuously upgrades its monitoring techniques.

6.4.4 The Need to Ensure the IT Infrastructure Better Promotes a Secure Environment

Criteria

Infrastructure configuration should promote a secure environment.

An organization should ensure that its infrastructure configuration is sufficient to support its security measures. The infrastructure includes not only the computers and networks, but also the connections between various locations.

With respect to the College's infrastructure configuration, we identified several opportunities to decrease the risk of unauthorized access to its systems. These were brought to management's attention in a separate report. Among the issues reported was the need to better segregate internal networks. Some of the College's publicly accessible

servers, including web servers and servers in academic departments, were connected directly to the College's internal network rather than being placed on a separate service network inside the firewall.

R19 We recommend that the College better segregate its internal network from publicly accessible servers.

COMMENTS OF OFFICIALS

The CS Department constantly evaluates, monitors, and maintains all aspects of computer security and has done an excellent job of protecting IT services to the College as well as providing a reasonably high level of security. All network access is assessed for risk and as time and resources permit, the CS Department upgrades or fine tunes access to all required systems.

Appendix A

Red River College
Critical IT Objectives, Strategies, Actions and Related Status

Objective 6: Integrate Information Technology in the delivery, operation, and management of all College programs and services.

Actions	Status (as at December 31, 2001)	Status		
		Satisfactory	Moderate	Preliminary
Strategy 6.1: Increase the extent to which technology is incorporated within the academic delivery process.				
• Expand the Teaching Learning Technology Centre (TLTC) with appropriate staffing, hardware and software to assist faculty in exploring and developing alternative means for delivering instruction and enhancing educational experiences using information technology.	• The evolution of the use of Web-CT has greatly expanded the level of support offered by the TLTC and 2,000 course hours have been offered by the TLTC. A half-time designer was also added to the supports offered the TLTC.	X		
• Implement a team-based approach to the development of course/portions of courses in alternative delivery formats.	• Implemented a team-based approach as part of online course development in 2000/01 and is further refining the approach in 2001/02. This will be incorporated into a set of guidelines for online courseware development at the College. • The project for re-structuring College programs focused on a common math program this past year and is now working on a common core set of courses in two divisions.	X		
• Deliver training to faculty in the use and application of information technology.	• The TLTC has offered approximately 5 sessions of training courses for a total of 2,000 staff training hours over the past year. • The College is organizing the delivery of an Instructional Systems Design workshop, as part of the process of building College capacity for online program/course development. • Program and Curriculum Development has also mounted two training sessions on project management to develop the skill set for curriculum development skills. • The model for Curriculum Validation includes a mentoring process for seconded faculty to ensure the development of curriculum development skills across the College.	X		
• Establish a mechanism to support employee access to or acquisition of hardware and software.	• This is being reviewed.	X		
Strategy 6.2: Increase the range of programs and services available on an e-commerce, e-business and e-learning basis.				
• Assess the opportunities and impacts of adopting e-business delivery methodologies.	• This is an ongoing activity in many areas of the College.	X		
• Establish a strategy to incorporate e-business and e-commerce techniques into the delivery of services.	• This is an ongoing activity involving reviews for opportunities.	X		
• Establish a strategy to provide the appropriate infrastructure for e-learning.	• Distance Education has received funding through the College Expansion Initiative and has advanced a second application as part of a 4 year plan.	X		

Appendix A
(cont'd.)

Red River College
Critical IT Objectives, Strategies, Actions and Related Status

Objective 6: Integrate Information Technology in the delivery, operation, and management of all College programs and services.

Actions	Status (as at December 31, 2001)	Status		
		Satisfactory	Moderate	Preliminary
Strategy 6.3: Establish a primary, reliable College communication system.				
• The College will move to electronic communication as its primary method of internal information dissemination.	• To enable a reliable College-wide communication system, the CS Department has been providing management support in areas that were not previously maintained by them. This allows the CS Department to standardize on systems and parameters. • The CS Department has assigned a staff member to work with Industrial Technologies to provide management and support. As the process and procedures are established in this area, other non-supported departments/divisions will be added. • The CS Department has been undertaking inventory of all systems to ensure that a standard version of software and hardware that will support reliable communication is in place.	X		
Strategy 6.4: Optimize the use of technology to improve administrative operations of the College.				
• Implement a corporate information system.	• Committees have been implemented to look at all issues with regards to the Student Information System. Additional committees are in place to look at Human Resources, Contacts and Timetabling/Scheduling.	X		
• Conduct a gap analysis of existing corporate systems with the current and future needs of the College.	• A survey was conducted to look at the gap between what is in place and what is available in a multitude of packages.	X		
• Purchase or develop the required software, hardware, training and installation for the new corporate system.	• Committees are working on requirements. This is a work in progress.	X		
• Provide readily available technical and program support to meet staff and students needs.	• The CS Department is developing more web access to support both staff and students. • Technical support is only available from 7:30am to 5:00pm weekdays and will not be increased unless more staff and resources are available.	X		
Strategy 6.5: Implement a plan to fund technology replacement/addition.				
• Develop a plan to add/replace/upgrade technology.	• The Chief Technology Officer produced a plan to "evergreen" desktops. Each year for 3 successive years, the College will lease 300 desktop computers. By the third and succeeding years, the College will be leasing 900 machines.	X		
• Instructors, students and corporate computer users will have access to adequate computing power convenient to their needs.	• Student's labs will be a part of the "evergreen" policy. This plan takes effect in 2001/02. Corporate users have had some upgrades to their systems based on department needs. A plan will be put forward to address the needs of the instructors and corporate users as a part of the "evergreen" policy.		X	

Appendix A
(cont'd.)

Red River College
Critical IT Objectives, Strategies, Actions and Related Status

Objective 6: Integrate Information Technology in the delivery, operation, and management of all College programs and services.

Actions	Status (as at December 31, 2001)	Status		
		Satisfactory	Moderate	Preliminary
Strategy 6.6: Annually review information technology.				
• Develop and implement a plan to annually review information technology.	• Information Technology is reviewed annually through the budget process. All CS Department supervisors report their requirements to the Chief Technology Officer.	X		
• Establish performance indicators.	• Information has been collected on performance indicators in preparation for developing the indicators at the College.		X	
• Compare performance indicators with other institutions.	• Documentation is being collected. Discussions have been initiated with other educational organizations in Manitoba.			X

Source: Actions/Strategies: Red River College's 5 Year Operational Plan (Actions/Strategies)
Status: Red River College Report "Progress in Achieving the Vision 2001" (Progress)

INFORMATION TECHNOLOGY ORGANIZATION

1.0 Executive Summary

1.1 BACKGROUND

Information technology (IT) refers to the resources, including software, hardware, networks, and telecommunications, which are used to provide automated processing of information and data. An alternative term is information and communications technology (ICT) which recognizes the convergence of information technology, telecommunications and data networking technologies into a single technology.

The process of defining the organization and relationships for the IT function helps to ensure that an entity receives the right IT services. The IT function should be organized to:

- Have staff members in sufficient numbers and skills;
- Have roles and responsibilities defined and communicated;
- Be aligned with the business;
- Facilitate the IT strategy for the entity; and
- Provide for effective direction and adequate control.

The Province recognizes the importance of defining the organization and relationships for the IT function. Accordingly, Treasury Board approved an organization review of information and communications technology in government. As a result, Internal Audit and Consulting Services of the Department of Finance undertook an initial scope review. Next, the Province engaged consultants who provided a report of options for an ICT governance model. Our review is designed to provide comments and recommendations that may assist the Province in its deliberations.

1.2 BEST PRACTICES REVIEW

As part of our review, we looked for best practices in organizing the IT function in general and for organizing IT management leadership in particular. We identified relevant standards developed by the Information Systems Audit and Control Association (ISACA) through its affiliated Foundation (ISACAF) and IT Governance Institute. ISACA is a professional organization representing individuals in more than 100 countries and comprising all levels of IT - executive, management, middle management and practitioner. ISACA fulfils the role of a central, harmonizing source of IT control practice standards recognized the world over. The standards are called the Control Objectives for Information and Related Technology (COBIT).

In addition, we identified guidance developed by the General Accounting Office (GAO) of the United States. The GAO is commonly called the investigative arm of the United States Congress. The GAO conducted research to determine how several leading organizations implemented their IT management leadership positions and supporting management infrastructures. They studied organizations from the public and private sectors, including senior governments. These organizations were selected as representing best practices for IT management based on awards and recognition from professional organizations and publications over several years.

As a result, the GAO developed guidance to assist government entities to effectively establish the IT management leadership role, commonly called the Chief Information Officer (CIO). However, the specific title and focus of the position can vary. The GAO guidance includes an Executive Guide titled, *"Maximizing the Success of Chief Information Officers, Learning from Leading Organizations".*

As well, we identified guidance developed by the National Association of Chief Information Officers (NASCIO) in the United States. NASCIO sponsored a 2002 study titled, *"Public-Sector Information Security: A Call to Action for Public-Sector CIOs".* While the focus of the study is security, guidance on IT governance is also included.

Also, we considered sources of best practice in Canada. The Information Technology Control Guidelines, published by The Canadian Institute of Chartered Accountants complements COBIT.

1.3 OBJECTIVE AND SCOPE

Our objective was to review the Provincial organization structure, including leadership, for managing IT regarding government Departments. Specifically, we reviewed the organization of IT in relation to the criteria that:

- A planning/steering committee oversees the IT function and its activities;
- Placement of the IT function in the Province's organization structure provides the appropriate level of authority to enable IT solutions and establishes a relationship with executive management to resolve IT issues;
- A framework exists for reviewing the IT organizational structure to meet objectives and changing circumstances;
- Responsibility has been assigned for a quality assurance function in IT;
- Responsibility has been assigned for the logical and physical security of the Province's information assets; and
- IT management maintains a coordination, communication and liaison structure between various interests inside and outside of the IT function.

These criteria are identified by the Control Objectives for Information and Related Technology (COBIT), as representing key contributing factors to a successful IT function. These criteria are supplemented with more detailed criteria identified by the General Accounting Office (GAO) in the United States as the practices of leading organizations.

Our review included interviews of officials and examinations of policies, procedures and other documentation conducted during the period May 2002 to February 2003.

The Department response indicates a number of actions they have taken subsequent to our fieldwork.

1.4 RECOMMENDATIONS

- That the Province establish a planning/steering committee to oversee the IT function and its activities.
- That the Province consider adopting an IT governance framework, such as the Control Objectives for Information and Related Technology (COBIT) from the Information Systems Audit and Control Foundation (ISACAF) and the IT Governance Institute. Such a framework can complement an ICT governance model of organization to be implemented. As well, COBIT can be used in conjunction with the IT Infrastructure Library approach to IT service management being promoted by the OIT.
- That the Province clarify the roles and responsibilities of IT management leaders, including the OIT and CIO, by:
    - identifying what business improvements the Province expects to accomplish through IT;
    - giving consideration to making the focus of the IT management leader (such as business strategist, policy and oversight manager, or operations specialist) consistent with the Province's mission, history, environment, culture and readiness to change;
    - ensuring that the IT management leader has the authority that is commensurate with the leader's role and responsibilities; and
    - giving consideration to defining the roles and responsibilities in legislation, similarly as is done by the Financial Administration Act or Civil Service Act for other functions.
- That the Province develop a performance measurement system for IT, with consideration given to recognized systems, such as *The Balanced Business Scorecard*.
- That the Province establish a quality assurance function for IT overall.

"The Balanced Business Scorecard-Measurements that Drive Performance", Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992

2.0 Introduction

2.1 BACKGROUND

Information technology (IT) refers to the resources, including software, hardware, networks, and telecommunications, which are used to provide automated processing of information and data. An alternative term is information and communications technology (ICT) which recognizes the convergence of information technology, telecommunications and data networking technologies into a single technology.

The process of defining the organization and relationships for the IT function helps to ensure that an entity receives the right IT services. The IT function should be organized to:

- Have staff members in sufficient numbers and skills;
- Have roles and responsibilities defined and communicated;
- Be aligned with the business;
- Facilitate the IT strategy for the entity; and
- Provide for effective direction and adequate control.

The Province recognizes the importance of defining the organization and relationships for the IT function. Accordingly, Treasury Board approved an organization review of information and communications technology in government. As a result, Internal Audit and Consulting Services of the Department of Finance undertook an initial scope review. Next, the Province engaged consultants who provided a report of options for an ICT governance model. Our review is designed to provide comments and recommendations that may assist the Province in its deliberations.

2.2 BEST PRACTICES REVIEW

As part of our review, we looked for best practices in organizing the IT function in general and for organizing IT management leadership in particular. We identified relevant standards developed by the Information Systems Audit and Control Association (ISACA) through its affiliated Foundation (ISACAF) and IT Governance Institute. ISACA is a professional organization representing individuals in more than 100 countries and comprising all levels of IT — executive, management, middle management and practitioner. ISACA fulfils the role of a central, harmonizing source of IT control practice standards recognized the world over. The standards are called the Control Objectives for Information and Related Technology (COBIT).

In addition, we identified guidance developed by the General Accounting Office (GAO) of the United States. The GAO is commonly called the investigative arm of the United States Congress. The GAO conducted research to determine how several leading organizations implemented their IT management leadership positions and supporting management infrastructures. They studied organizations from the public and private sectors, including senior governments. These organizations were selected as representing best practices for IT management based on awards and recognition from professional organizations and publications over several years.

As a result, the GAO developed guidance to assist government agencies to effectively establish the IT management leadership role, commonly called the Chief Information Officer (CIO). However, the specific title and focus of the position can vary. The GAO guidance includes an Executive Guide titled, *"Maximizing the Success of Chief Information Officers, Learning from Leading Organizations".*

As well, we identified guidance developed by the National Association of Chief Information Officers (NASCIO) in the United States. NASCIO sponsored a 2002 study titled, *"Public-Sector Information Security: A Call to Action for Public-Sector CIOs".* While the focus of the study is security, guidance on IT governance is also included.

Also, we considered sources of best practice in Canada. The Information Technology Control Guidelines, published by The Canadian Institute of Chartered Accountants complements COBIT.

2.3 ORGANIZATION OF THE IT FUNCTION FOR DEPARTMENTS

An organization chart for managing IT regarding government Departments is included in **Appendix A**. A schedule of roles, responsibilities, and authorities for information technology is included in **Appendix B**. Since June 2000, the Office of Information Technology (OIT) has gone through extensive organizational change. As well, the Coordinated Services Committee and Unit have initiated an organization review of information and communications technology in government.

The following figures indicate the extent of these resources devoted to the IT organization of Departments:

- As at March 31, 2002 the recorded capital cost of computer hardware and software assets used by Government Departments was just over $210 million, an increase of $ 37 million from March 31, 2001.
- For the year ended March 31, 2002 the Government Departments spent about:
    - $10 million on acquiring miscellaneous computer hardware and software that was expensed and not included in assets;
    - $4 million for leasing computer hardware;
    - $48 million on various computer related services, primarily service provider fees for managing desktop computers and fees for a wide area computer network;
    - $16 million for consulting services regarding IT; and
    - $24 million in payroll costs for over 440 employees in the information technology classification series.

3.0 Objective and Scope

Our objective was to review the Provincial organization structure, including leadership, for managing IT regarding government Departments. Specifically, we reviewed the organization of IT in relation to the criteria that:

- A planning/steering committee oversees the IT function and its activities;
- Placement of the IT function in the Province's organization structure provides the appropriate level of authority to enable IT solutions and establishes a relationship with executive management to resolve IT issues;
- A framework exists for reviewing the IT organizational structure to meet objectives and changing circumstances;
- Responsibility has been assigned for a quality assurance function in IT;
- Responsibility has been assigned for the logical and physical security of the Province's information assets; and
- IT management maintains a coordination, communication and liaison structure between various interests inside and outside of the IT function.

These criteria are identified by the Control Objectives for Information and Related Technology (COBIT), as representing key contributing factors to a successful IT function. These criteria are supplemented with more detailed criteria identified by the General Accounting Office (GAO) in the United States as the practices of leading organizations.

Our review included interviews of officials and examinations of policies, procedures and other documentation conducted during the period May 2002 to February 2003.

The Department response indicates a number of actions they have taken subsequent to our fieldwork.

4.0 Findings and Conclusions

4.1 IT PLANNING/STEERING COMMITTEE

Best practices indicate that there should be a planning/steering committee to oversee an IT function and its activities. Committee membership normally includes representation from senior management, user management and the IT function. Such a committee would meet regularly and report to senior management. As well, a key role of such a committee would be to direct the strategic planning process for IT. The activity of aligning IT plans with those of the business is missing or poorly addressed in many organizations. The planning/steering committee provides the vital coordination of all business plans, projects, and programs with IT plans, projects, and programs.

Findings

- The Coordinated Services Committee was created originally for the purpose of providing direction and management for the development and delivery of the Province's Internet Web site. Also, the Coordinated

Services Unit was established to provide staff support to the Committee in the areas of policy development, content coordination, and strategic direction. However, the Coordinated Services Committee and Unit have evolved to being engaged in a review of information and communications technology in government for the purpose of implementing an effective ICT governance model. Currently, the Province has not established a planning/steering committee to oversee the IT function and its activities.

Conclusion

- *The absence of an IT planning/steering committee exposes the Province to an undue risk that IT activities will not be aligned with overall government objectives, that IT funding will be misallocated, and that strategic plans for IT will fail to support key government plans in an optimal manner.*

4.2 ORGANIZATIONAL PLACEMENT OF IT FUNCTION

Best practices indicate that an IT function should have the authority and the independence from user organization units to the degree necessary to determine effective IT solutions and implement the solutions. In other words, IT management leadership is positioned with the ability to strategically view and apply IT to the best advantage of the entity. Also, the IT function should establish a partnership with top management to help increase awareness, understanding and skill in identifying and resolving IT issues. We examined the placement of IT against the following detailed criteria that:

4.2.1 An IT management leader position is established.
4.2.2 The role and responsibilities of the IT management leader are clearly defined.
4.2.3 The IT management leader has sufficient authority.

4.2.1 IT Management Leader

Larger organizations generally recognize the importance of information by establishing the position of IT management leader, commonly called Chief Information Officer (CIO). Often the IT management leader is responsible for IT planning, under the direction of a senior committee. The CICA IT Control Guidelines specify that the role of the IT management leader is to oversee the following:

- Development of IT policies and standards;
- Development and maintenance of an IT strategic plan;
- Coordination of the development of an information systems security architecture
- Provision of technical support to IT owners, custodians, and users; and
- Direction of centralized IT services.

Findings

- In 1998, Treasury Board approved the establishment of the Office of Information Technology (OIT) headed by a CIO at the Deputy Minister level. However, in 2000, the function of the OIT began to be reassessed.

The classification of the CIO position was reduced and an Acting CIO was appointed June 5, 2000. Then, a committee of senior officials undertook to review and make recommendations regarding the ongoing role and operations of the OIT. Next, the Treasury Board approved an organization review to develop an ICT governance model. The model has not yet been implemented.

Conclusion

- *The delay in implementing an effective approach to ICT governance hampers the ability of staff members to function effectively.*

4.2.2 Roles and Accountability for the IT Management Leader

The GAO guidance states that senior executives need to consider the role of IT and how vital it is to accomplishing business objectives. They need to examine how IT and IT management can help meet business needs. They should define the objectives for improving business, specifically what they expect to accomplish through IT.

Moreover, an entity should ensure that all personnel in the organization have and know their roles and responsibilities in relation to information systems. Leading organizations clearly define and document the role and responsibilities of the IT management leader, or CIO, particularly in relation to other senior managers.

Findings

- There is a lack of government-wide directives defining the roles and responsibilities regarding IT management leadership, such as the OIT and the CIO. For example, there is no legislation related to the management of IT. Such legislation exists for other functions, such as financial management, human resource management, and purchasing. We understand that the role and operations of the OIT, and other IT related groups, have been under review for the past two and a half years.

Conclusion

- *The role and responsibilities for IT management leadership are not clearly defined.*

4.2.3 Authority of the IT Management Leader

All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Leading organizations ensure that the IT management leader has the authority needed to be effective. The IT management leader reports to the head of the organization and is involved in strategy discussions at the highest level, in order to lead the organization in using IT to corporate advantage. The IT management leader is empowered to work with other senior executives to discuss and decide among alternative IT products and strategies for meeting business needs. The IT management leader has a key role in IT investment decision-making, or has budget control, or has executive management backing for IT programs and initiatives.

Findings

- A review of the organization chart for IT indicated that the responsibility for managing IT in the Province is dispersed. The organization chart is included as Appendix A. There is no government Department or Minister whose primary responsibility is IT. The senior managers for the IT function are below the Deputy Minister level. For example, the OIT and CIO formerly reported to the Secretary to Treasury Board, but now report to the Deputy Minister of Energy, Science and Technology. Some important IT related organization groups, such as Desktop, Telecommunication and Network Services, report to managers who have primary responsibilities other than IT.

- During 2001 and 2002, the OIT mandate was to provide leadership, stewardship, and facilitation, but the OIT and CIO lack direct authority over many IT personnel and activities. Instead the OIT sought to cultivate co-operation and co-ordination between Departments and agencies by working with program managers and IT directors. In the autumn of 2002, the new Department of Energy, Science and Technology was created. The OIT is now part of this new Department and is responsible for overseeing the strategic use of IT resources for the Province

- On the other hand, the IT function is organized similarly to that of many other Canadian provinces and territories. We reviewed the CIO organizations in other Canadian jurisdictions. Our review was based on the Internet Web sites maintained by those organizations. The results of our review are included as Appendix B. Currently, two Provinces appear to have a CIO at the Deputy Minister level. In contrast, NASCIO, representing Chief Information Officers of the American States, reported in 2001 that 25 states have a CIO reporting directly to the State Governor and the number is on the increase.

"The Role of the State Chief Information Officer", NASCIO, January 2001

- Furthermore, a NASCIO study on public sector information security reported that a growing number of states are moving toward a roles-based arrangement. The roles-based model usually has a central executive council with broad-based representation. The council is responsible for policies, long-range plans, project-management standards, and enterprise architecture. A chief information technology architect, working with agencies, prepares architectures, long-range plans, policies, and project management standards. The CIO occupies a cabinet-level position and implements these enterprise plans, policies, and project management standards. However, the United States has a form of government that differs from the form of government in Canada.

Conclusion

- *Unlike leading organizations and pending the implementation of an effective ICT governance model, the Province lacks an IT management leader with the authority to lead the Province in using IT to government-wide advantage.*

4.3 REVIEW OF ORGANIZATIONAL ACHIEVEMENTS

A framework should be in place for reviewing and revising the organizational structure in order to meet objectives and changing circumstances. Services to be delivered by the IT function should be measured by management and be compared with target levels. Assessments of the IT function should be performed on a continuous basis.

Findings

- The Province has not developed a performance measurement system in general or for IT in particular. Consequently, measures, such as performance indicators, have not been developed for the IT function on a government-wide basis.

Conclusion

- *The lack of a performance measurement system increases the risk that the objectives for IT will not be met.*

4.4 QUALITY ASSURANCE FUNCTION

Management normally assigns the responsibility for the performance of the quality assurance function to staff members of an IT function. Also, management ensures that appropriate quality assurance, systems, controls and communications expertise exist in an IT function's quality assurance group. The organizational placement within the IT function and the responsibilities and the size of the quality assurance group should satisfy the requirements of the organization.

Findings

- The Province has an initiative to improve how Manitoba citizens can access provincial government information and services, including the use of ICT. This initiative is concerned with measuring the quality of service provided. Also, the OIT is promoting the IT Infrastructure Library (ITIL) approach to IT service management. ITIL is a widely accepted approach that provides a comprehensive set of best practices to IT service management.
- Also, some major IT initiatives undertaken by the Province have had a quality assurance function. We did not verify whether Departments have a quality assurance function for specific IT development projects. However, the Province does not have an overall quality assurance function for IT.

Conclusion

- *The lack of a quality assurance function increases the risk that information systems will not meet user needs.*

4.5 RESPONSIBILITY FOR LOGICAL AND PHYSICAL SECURITY

Management formally assigns the responsibility for assuring both the logical and physical security of the organization's information assets to an information security manager, reporting to the organization's senior management. At a minimum, security management responsibility is established at an organization-wide level to deal with overall security issues in an organization. If needed, additional security management responsibilities are assigned at a system specific level to cope with the related security issues.

Findings

- In 1999, the Province established the Information Protection Centre (IPC). The IPC is responsible for dealing with overall computer security issues at a government-wide level. Also, Departments have security coordinators, who deal with computer security issues at a specific information system level.
- Moreover, the Province has a branch that deals with physical security of government buildings and property. As well, there is an insurance and risk management branch that deals with security risks at a government-wide level.
- In addition, the Province has an archives branch to deal with government records, including requirements under the Freedom of Information and Protection of Privacy Act (FIPPA). Furthermore, there are designated FIPPA coordinators in each government Department and agency.

Conclusion

- *Responsibility has been assigned for assuring both the logical and physical security of the information assets.*

4.6 RELATIONSHIPS

IT management normally establishes and maintains an optimal coordination, communication and liaison structure between various interests inside and outside of the IT function. Such interests include users, suppliers, security officers, and risk managers.

Findings

- A number of measures exist to promote relationships on a government-wide level between the IT function and various interests. These measures include the following:
    - The OIT and CIO liaise with the Information Technology Council (ITC). The ITC consists of the most senior information technology professional from each Department. The ITC mission indicates that it generates a consensus voice on issues of IT importance to the government and meets to assist one another on Departmental operations and development activities.
    - The OIT reviews the IT plans of Departments, including the development of new information systems.

- The IT Business Planning section within OIT has been working with the Insurance and Risk Management Branch of government.
- Desktop, Telecommunication & Network Services liaises with both the Desktop Advisory Council, whose members represent IT Directors from Government Departments, and with the Desktop Coordinator User Group, whose members represent computer users from the Departments.
- The Information Protection Centre, which is part of the OIT, liaises with the security coordinators for each Department.
- Periodic "open house" events are held to provide information to government staff members within and outside of the IT function. These events also include some supplier representatives.

Conclusion

- *IT management is undertaking actions to establish and maintain a coordination, communication and liaison structure between various interests inside and outside of the IT function.*

5.0 Recommendations

- That the Province establish a planning/steering committee to oversee the IT function and its activities.
- That the Province consider adopting an IT governance framework, such as the Control Objectives for Information and Related Technology (COBIT) from the Information Systems Audit and Control Foundation (ISACAF) and the IT Governance Institute. Such a framework can complement an ICT governance model of organization to be implemented. As well, CobiT can be used in conjunction with the IT Infrastructure Library approach to IT service management being promoted by the OIT.
- That the Province clarify the roles and responsibilities of IT management leaders, including the OIT and CIO, by:
  - identifying what business improvements the Province expects to accomplish through IT.
  - giving consideration to making the focus of the IT management leader (such as business strategist, policy and oversight manager, or operations specialist) consistent with the Province's mission, history, environment, culture and readiness to change.
  - ensuring that the IT management leader has the authority that is commensurate with the leader's role and responsibilities.
  - giving consideration to defining the roles and responsibilities in legislation, similarly as is done by the Financial Administration Act or Civil Service Act for other functions.

"The Balanced Business Scorecard-Measurements that Drive Performance", Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992

- That the Province develop a performance measurement system for IT, with consideration given to recognized systems, such as the Balanced Business Scorecard.
- That the Province establish a quality assurance function for IT overall.

Departmental Response

The Coordinated Services Unit undertook a review of the current state of ICT (from a corporate strategy and delivery perspective) in the fall of 2002 and provided recommendations to Treasury Board in December 2002.

The recommendations were approved with direction to implement the proposed governance option.

This option significantly reorganizes the ICT services provided on a government-wide basis. It gives the central organization authority to approve department plans, and provides it with the teeth necessary to optimize ICT assets across government. This approach provides for an emphasis on government-wide optimization, rather than optimization at a departmental level, and provides for tight control over ICT expenditures and a great degree of standardization.

It also provides CSU the ability to develop a coordinated approach to customer service.

In specific response to the recommendations suggested within the Auditor General's report, a number of them have already been achieved:

- *There is already an established senior Deputy Minister Committee (Coordinated Services Committee) in place that among other things oversees the IT function and its activities. As well, the central ICT organization that has been created (Manitoba Information and Communications Technology) reports through a Deputy Minister within the newly formed Department of Energy, Science and Technology.*
- *An ICT governance structure has been proposed and approved for implementation in the 2003/04 Estimates.*
- *Three of the four organizations (DTN&S, ESM, OIT) are already implementing the IT Infrastructure Library (ITIL) approach to IT service management to some degree.*
- *As part of the implementation of the recommended governance option, clarification of the roles and responsibilities of IT management leaders (at the corporate level) is being established and will be communicated throughout the government departments.*
- *To some degree the ITIL approach will guide the service management processes to include performance measurements and quality assurance systems. These processes and performance management and quality*

systems will become standard practice, and will be promoted throughout government IT functional areas as standards.

Throughout the ICT review phase, a number of the issues identified within the Auditor General's report were found and accounted for in developing the recommended governance proposal.

As the new governance structure is implemented and the organization moves further forward with transitioning from separate corporate service entities to a single coordinated service organization, it is expected that process improvements, reduction of duplicative functions and service improvements will be identified and put in place.

Increasingly, citizen-centric service has become a priority goal of and throughout the provincial government. This is evidenced through initiatives such as the Coordinated Services Initiative (At Your Service Manitoba) which focuses on improving access points and response times for citizens, and other consumers, to government services and information through a multi-channel service delivery approach. This then necessitates that government-wide service standards and performance measurements (for both public service delivery and internal processes) are developed and monitored to ensure that we meet our goals of improved access and service delivery.

Through the 2003/04 Estimates, authorization was requested and granted for the creation of a central ICT organization named Manitoba Information and Communications Technologies (MICT).

This organization merged four former ICT organizations (BSI, DTN&S, ESM, OIT) and operates with three branches; namely ICT Strategy, Planning & Analysis, ICT Service Delivery and Management Services. In fact, the individual organizations no longer exist although the reports continue to refer to them.

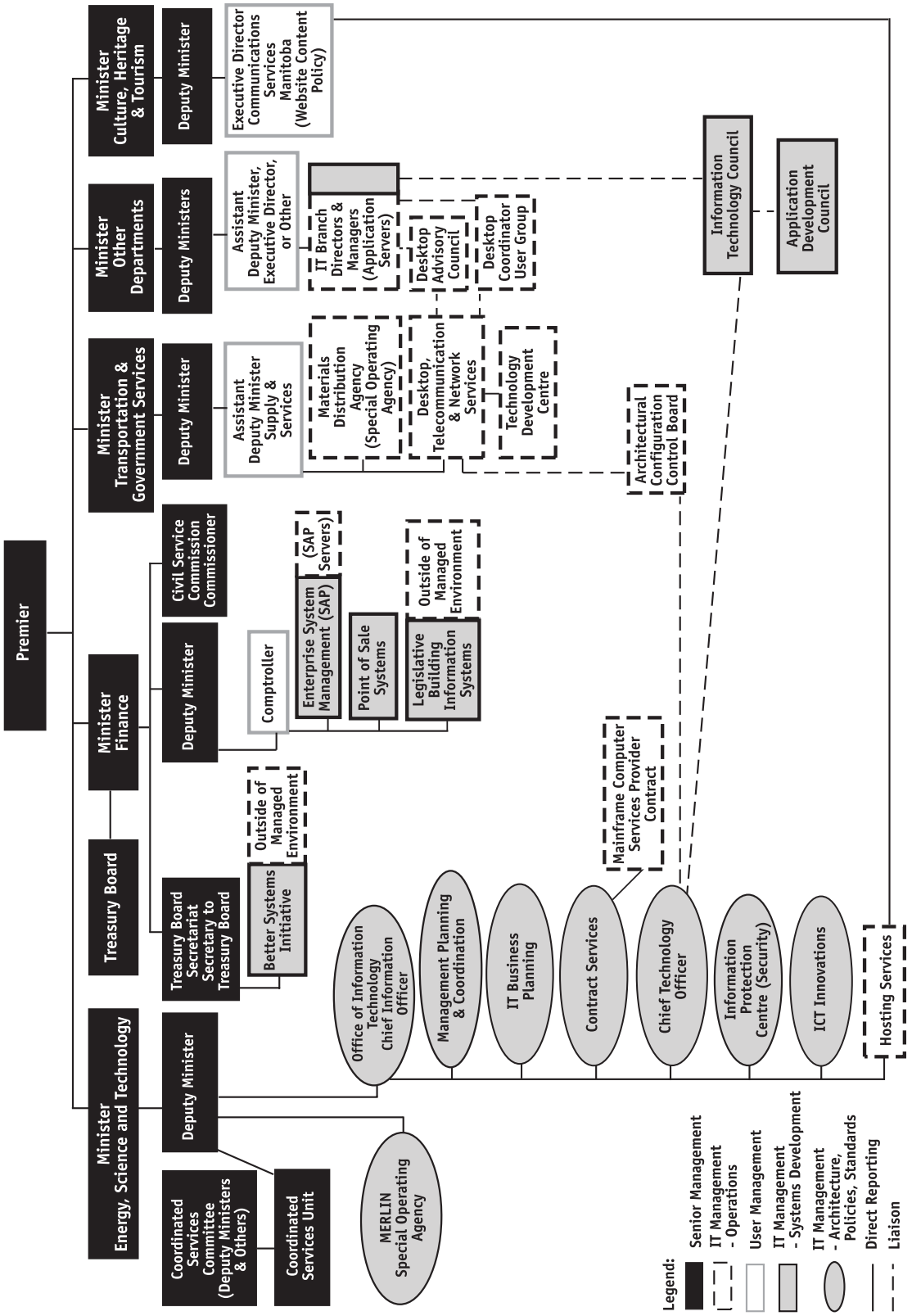
Key drivers which continue to influence the direction of the new MICT division include:

- *ensuring corporate coordination and relevance with government policy for key concurrent initiatives and opportunities (SAP, Desktop Refresh, Health IT Initiatives);*
- *infrastructure consolidation and economies of scale;*
- *standardizing IT best practices;*
- *maximizing government's buying power; and*
- *re-orientation of the previous internally focused mandate and priorities of Manitoba's IT programs towards a model of citizen-centric service.*

As for the departmental ICT units, the Deputy Ministers' Expenditure Management Committee has requested a series of options to re-organize the delivery of strategic and operational Information and Communications Technology (ICT) service to departments in government. These activities will lead to further organization changes in the delivery of ICT in government.

Appendix A

PROVINCE OF MANITOBA - ORGANIZATION CHART FOR INFORMATION TECHNOLOGY



Appendix B

SCHEDULE OF ROLES, RESPONSIBILITIES, AND AUTHORITY FOR INFORMATION TECHNOLOGY

Based on Review of Annual Reports, Supplementary Information for Legislative Review, Manitoba Government Intranet and Internet Sites

Treasury Board

Role

Treasury Board is a committee of Executive Council (Cabinet). The Minister of Finance is the Chair of Treasury Board. Treasury Board is the decision-making body responsible for reviewing the expenditure and revenue plans of all departments and agencies funded through the annual revenue and expenditure estimates process of government.

Responsibilities

Treasury Board is responsible for:

- Government-wide management practices and systems
- Government fiscal management and control, including the management and control of expenditures and revenues
- Approving the organization of government departments and the staffing complement and spending levels required for the delivery of government programs

Authority

The Financial Administration Act established Treasury Board and specifies its responsibilities and authority.

Coordinated Services Committee and Coordinated Services Unit

Role

The Coordinated Services Committee is comprised of senior management persons, including several deputy ministers, as well as senior staff from the Coordinated Services Unit. The mandate of the Committee is to review the information technology requirements of the government, including e-commerce.

The Coordinated Services Unit was created to support the work of the Committee and implement its initiatives. A Director heads the Unit. The priority task of the Unit is to bring together the three main ways citizens get information, request services, or actually receive services from the Provincial government:

- Internet
- Telephone
- In Person

Responsibilities

The Committee and Unit are responsible for:

- Improving the coordination of efforts across government in the area of information and communications technology.

Appendix B
(cont'd.)

- Conducting a review to provide corporate vision, direction, and priorities for the Web activities of the government, as well as examine the governance models and systems of delivery and planning in information and communication technology.

Authority

In February 2000, the Minister of Finance announced the establishment of an information technology review committee, as a result of the review by consultants of major information technology initiatives. This committee evolved into the Coordinated Services Committee. Both Treasury Board and the Community Economic Development Committee of Cabinet have approved the current review of ICT governance.

The Coordinated Services Unit was created by Executive Council (Cabinet) in 2002.

Department of Finance

Treasury Board Secretariat

Role

The Treasury Board Secretariat provides financial and analytical support and advice to the Minister of Finance and Treasury Board. A Deputy Minister who acts as Secretary to the Board heads the Secretariat.

Responsibilities

The major functions fulfilled by the Treasury Board Secretariat include:

- Planning and coordinating the review and preparation of the annual estimates and participating in the development of the annual budget
- Providing analyses in support of the efficient and effective utilization/ allocation of the province's financial and human resources, both in the context of the annual estimates process and on an ongoing basis throughout the year
- Providing guidance to departments on a government wide planning and performance measurement initiative.

Authority

Treasury Board Secretariat acts on behalf of Treasury Board.

Better Systems Initiative

Role

The Better Systems Initiative (BSI), Development & Deployment (D&D) champions the development of e-business technologies and applications in accordance with the vision for electronic services in the government. Also, BSI is a centre of best practices.

An Assistant Deputy Minister leads BSI, while Project Directors are responsible for specific components of BSI. In addition, there is a BSI Advisory Committee which includes the CIO and Deputy Ministers from mainly departments with electronic service applications/ projects. The BSI Advisory Committee monitors progress, makes strategic decisions, and communicates with Ministers, as well as Deputy Ministers not on the Committee.

Appendix B
(cont'd.)

Responsibilities

The responsibilities of BSI include:

- Initiate and execute corporate electronic service projects
- Develop and implement guidelines and standards based on the overall enterprise architecture
- Establish a pool of highly skilled resources and capabilities to serve in a consulting capacity to electronic service projects
- Create and maintain a operating environment that supports access to electronic services on a continuous basis

Authority

In 1995, BSI was established as a pilot project to champion the e-government revolution in the provincial government. In 1997 Treasury Board approved BSI as one of several initiatives to improve the government's ability to deliver service.

Enterprise System Management

Role

Enterprise System Management (ESM) manages the enterprise-wide computer system that provides integrated finance, procurement, human resources, and payroll applications. An Executive Director, who reports to the Comptroller, heads ESM.

Responsibilities

The responsibilities of ESM include the following:

- Maintaining and enhancing the functionality of the enterprise-wide management information system, including the physical computer facilities
- Maximizing the overall value of the system functions
- Providing training to users

Authority

ESM was established in the fiscal year ended March 31, 2000 as part of the Department of Finance, which specifies its responsibilities and authority with the concurrence of Treasury Board. ESM was established as a result of the Better Methods Initiative that implemented the enterprise-wide computer system.

Legislative Building Information Systems

Role

The Legislative Building Information Systems (LBIS) branch provides complete information technology services to all users in the Legislative Building. Users comprise both government and non-government staff members. A Director, who reports to the Comptroller, heads the branch.

Appendix B
(cont'd.)

Responsibilities

The responsibilities of the branch include the following:

- Providing desktop computer services, including the computer network infrastructure
- Implementing and supporting custom business applications
- Maintaining a computing environment that reflects best practices in security
- Maintaining business continuity and disaster recovery plans

Authority

LBIS was established many years ago as part of the Department of Finance, which specifies it responsibilities and authority with the concurrence of Treasury Board.

Architectural Configuration Control Board

Role

The Architectural Configuration Control Board (ACCB) acts to ensure that changes to the information technology infrastructure of government are allowed only if consistent operational capabilities are maintained. The ACCB ensures that the infrastructure remains consistent regarding performance as well as functional and physical attributes. The infrastructure comprises the provincial data network, the desktop managed environment, the IPC, ManWeb, and the application servers maintained by departments.

The Chief Technology Officer chairs the Board which includes representatives from the Information Protection Centre and Desktop, Telecommunication and Network Services.

Responsibilities

The ACCB is responsible for:

- Reviewing all proposed changes to the information technological infrastructure
- Approving only necessary changes
- Ensuring that only approved changes are implemented
- Ensuring that the implemented changes are properly documented

Authority

In January 2000, Treasury Board authorized the ACCB to act on behalf of OIT as the technical change manager for the Province's information technology infrastructure.

Department of Energy, Science and Technology

Office of Information Technology

Role

The objective of the Office of Information Technology (OIT) is to develop and implement information technology strategies that will improve government operations and deliver better service to the citizens of Manitoba. The Chief Information Officer (CIO), who reports to the Deputy Minister, heads OIT.

Appendix B
(cont'd.)

The Chief Technology Officer, who oversees the planning and design of government's enterprise-wide technology architecture and infrastructure, reports to the Chief Information Officer.

Responsibilities

OIT is responsible for overseeing the use of ICT resources for the Government of Manitoba and this responsibility is met by focusing on three key areas:

- Developing corporate policies, strategies, architectures and standards
- Aligning organizational IT efforts with Manitoba's ICT vision and direction
- Delivering core ICT services

Authority

Treasury Board approved the establishment of OIT during the fiscal year ended March 31, 1999 to support the Chief Information Officer. OIT was transferred from the Department of Finance to the Department of Energy, Science and Technology in September 2002.

Information Protection Centre

Role

In November 1999, the Information Protection Centre (IPC) was created as part of the Office of Information Technology. A Director who reports to the CIO heads the IPC. The IPC ensures that government computer networks remain secure yet open, accessible and reliable.

Responsibilities

The IPC mission is as follows:

- To protect the government's networks by continuing to find and address vulnerabilities in networked computers and systems and thereby improve the government's overall security baseline
- To detect misuse of, or attacks against, the government's networks and respond to minimize the impact of these security incidents
- To provide assistance to correct deficiencies in system configuration
- To provide a single point of contact for network security within the government

Authority

Treasury Board approved the establishment of the IPC to manage the security infrastructure of the government but did not specify the authority of the IPC in regards to security incidents. In practice, the IPC acts to protect the security of the government computer networks.

Hosting Services

Role

As part of OIT, Hosting Services manages and coordinates Internet and Intranet services across the government. Hosting Services hosts the government Web sites on both the Internet and the government Intranet. A Director, who reports to the CIO, heads Hosting Services.

Appendix B
(cont'd.)

Responsibilities

Hosting Services is responsible for:

- Development of Web-related strategies, policies, procedures and technical standards
- Coordination of Web projects
- Hosting the government's Internet and Intranet services

Authority

Treasury Board approved the establishment of Hosting Services in 1999. Hosting Services acts as the service provider for the Communications Services Manitoba division of the Department of Culture, Heritage and Recreation. The Public Printing Act specifies the responsibilities and authority of Communications Services Manitoba.

Manitoba Education Research and Learning Information Networks

Role

The Manitoba Education Research and Learning Information Networks (MERLIN) provides direction and management in the use of technological tools, such as computer networks, to improve educational services to learners. The learners are primarily students from kindergarten to senior four.

Responsibilities

The responsibilities of MERLIN include the following, primarily for the kindergarten to senior four community:

- Develop and institute technology standards
- Provide training to school divisions, including support for distance education applications
- Provide Internet services
- Provide audio conferencing services
- Assist in Province-wide purchasing and licencing of hardware and software

Authority

MERLIN was established in April 1995 as a special operating agency under the authority of the Department of Education, Training and Youth. The Special Operating Agencies Financing Authority Act provides for the establishment of special operating agencies. These agencies are granted more direct responsibility for their operating results and have increased management flexibility to encourage entrepreneurship, enhance service, and reduce the cost to government

Department of Transportation and Government Services

Desktop, Telecommunication and Network Services

Role

Desktop, Telecommunication and Network Services (DTNS) administers the Desktop Management Program. This program primarily involves a service provider who manages

Appendix B
(cont'd.)

the computers, printers and standard software used by government personnel, as well as the computer servers that provide printing, e-mail, and other local area network services. Also, the service provider provides help desk support, as well as education and training services to Provincial personnel. This arrangement is commonly referred to as the "managed environment."

In addition, DTNS centrally manages the telecommunication and radio services for the government. These services include telephones, two-way radios, photocopiers, facsimile machines, as well as administering the contract with service provider who provides and manages the provincial data network linking departments, agencies and other operations. The data network also includes dial-in and satellite computer connections.

A Director who reports to the Assistant Deputy Minister for Supply and Services heads DTNS.

Responsibilities

The responsibilities of DTNS include the following:

- Reduction of information technology infrastructure costs through aggregation, integration, and standardization of desktop computer and telecommunication services
- Achieving operating efficiencies and cost control for the information technology infrastructure
- Assessing the value to government of desktop computer and telecommunication services
- Provision of radio communication services to government
- Service levels and pricing as well as cost recovery mechanisms that are effective and meaningful for clients

Authority

DTNS was formed in the fiscal year ended March 31, 2002 within the Department of Transportation and Government Services by merging Desktop Management Services and Telecommunication Services Branch. DTNS operates in accordance with initiatives approved by Treasury Board, such as the Desktop Management Program, and under the general authority of The Government Purchases Act

Technology Development Centre

Role

The Technology Development Centre (TDC) provides facilities for departments to test computer application software and hardware before introducing these products into the government operational environment. The TDC also has facilities for conducting computer-based training or application software development. Staff members from DTNS operate the TDC.

Responsibilities

The TDC provides testing facilities that replicate the information technology infrastructure environment of the government.

Appendix B
(cont'd.)

Authority

The TDC was established by DTNS to promote proper testing of computer products before introducing them into the government computer environment. However, departments and agencies are not required to use the facilities provided by the TDC.

Desktop Coordinator User Group

Role

The Desktop Coordinator User Group provides a forum for user representatives to address issues regarding the "managed environment." This environment refers to the arrangement for providing basic computer services to Department employees. This arrangement includes the involvement of a service provider.

Responsibilities

The responsibilities of the User Group include meeting with representatives of Desktop, Telecommunications and Network Services, as well as the service provider.

Authority

The Desktop Coordinator User Group is a peer group and has no specific authority.

Materials Distribution Agency

Role

The Materials Distribution Agency (MDA) fulfills the purchasing function on behalf of departments for a variety of products. A Chief Operating Officer heads the MDA.

Responsibilities

The MDA has the following responsibilities:

- Maintain a two business day turnaround on 98% of urban orders and four business day turnaround on rural orders
- Maintain stocked response rates to greater than 99% of all items ordered
- Continue to produce and distribute a catalog and news flyers on new products, as well as market services to Regional Health Authorities

Authority

In 1974, the MDA was created as a branch of the government services department. On April 1, 1993 the MDA commenced operations as a special operating agency. It currently operates under the authority of the Department of Transportation and Government Services. The Special Operating Agencies Financing Authority Act provides for the establishment of special operating agencies. These agencies are granted more direct responsibility for their operating results and have increased management flexibility to encourage entrepreneurship, enhance service, and reduce the cost to government.

Appendix B (cont'd.)

Department of Culture, Heritage and Tourism

Communications Services Manitoba

Role

Delivers communication and information services to the public and to government departments. An Executive Director heads this Division.

Responsibilities

The Business Services branch is responsible for:

- Liaisons with government departments and the Office of Information Technology on the development and presentation of content on the Government of Manitoba Internet Web site

Authority

The Public Printing Act specifies the responsibilities and authority of the Communications Services Manitoba in regards to the content, visual appearance and display of documents electronically on Intranet and Internet Web sites.

All Departments

Information Technology Council

Role

The Information Technology Council (ITC) is forum for information technology directors from departments to discuss issues. The directors elect a Chairperson annually.

Responsibilities

The ITC mission is as follows:

> To maintain a peer group of information technology professionals from the line departments that generates a consensus voice on issues of information technology importance to the Government of Manitoba and meets to assist each other on their respective departmental operations and development activities.

Authority

The ITC was established in 1994 as a peer group. The ITC has no specific authority. Members of the ITC have the authority of their positions as information technology directors/managers in departments.

Application Development Council

Role

The Application Development Council (ADC) works to facilitate the exchange of information to promote the:

- Minimal deployment of competing and overlapping technologies
- Establishment of a repository of best practices for software development

Appendix B
(cont'd.)

Responsibilities

The responsibilities of the ADC include:

- Maintaining a schedule indicating the usage in Departments of software development language/products

Authority

The ADC was established in January 2000 as a subcommittee of the ITC.

Desktop Advisory Council

Role

The Desktop Advisory Council works in cooperation with Desktop, Telecommunication and Network Services to provide advice and input into the issues and processes required for the "management environment." The managed environment refers to the arrangement for providing basic computer services to Department employees. This arrangement includes the involvement of a service provider.

Responsibilities

The responsibilities of the Desktop Advisory Council include attending meetings with Desktop, Telecommunication and Network Services.

Authority

The Desktop Advisory Council was established in November 2001 as a subcommittee of the ITC.

Department Information Technology Branches

Role

In general, a departmental information technology branch develops and manages computer application systems and supporting technology for the department, including plans for the department's use of information technology. A manager or director heads each branch.

Responsibilities

In general, an information technology branch has the following responsibilities:

- Develop annual systems plans that are approved by OIT
- Maintain and enhance existing systems and technology to ensure that they continue to meet business needs
- Develop and implement new systems and technology to support department business needs

Authority

The information technology branch is established by each department, which specifies it responsibilities and authority with the concurrence of Treasury Board.

Appendix B
(cont'd.)

Civil Service Commission

Role

The Civil Service Commission is an independent and impartial agency of government that develops and delivers human resource management services. The Executive Office manages and directs the Commission. The Human Resources Management Division supports human resource management programs, policy and procedures across government. A Commissioner with the status of Deputy Minister heads the Commission. The Commissioner reports to the Minister responsible for the Civil Service Act.

Responsibilities

The responsibilities of the Executive Office include the following:

- Managing the human resource function in accordance with The Civil Service Act and responding to government policy and supporting the goals of departments and the government
- Developing strategic initiatives and programs

The responsibilities of the Human Resources Management Division include the following:

- Reviewing and developing policies related to staffing, employment equity, human resource planning and assessment
- Maintaining and enhancing the corporate human resource policy manual
- Support and enhance the human resource information component of the enterprise-wide computer system that provides management information

Currently, there is no specific program relating to information technology staffing.

Authority

The Civil Service Act specifies the responsibilities and authority of the Commission.

Appendix C
(cont'd.)

ANALYSIS OF CHIEF INFORMATION OFFICER (CIO) ORGANIZATIONS BY JURISDICTION

(Based on Review of Internet Web Sites Maintained by Jurisdictions)

Jurisdiction	Strategic Planning or Steering Committee	CIO Title	CIO Unit	Location of CIO Unit	Report To	CIO Unit Role and Relation to Departments
Canada	Not identified	Chief Information Officer	Chief Information Officer Branch	Treasury Board	Secretary of the Treasury Board (Comptroller General) and two Associate Secretaries	Provide leadership, coordination and broad direction. Serve as technology strategist. Facilitate enterprise-wide solutions.
British Columbia	Premier's Technology Council (Premier is Chair and members are from the private sector.)	Deputy Minister and Chief Information Officer	Chief Information Office	Office of the Premier	Minister of Management Services	Provide leadership and strategic direction. Responsible for governance framework, including legislation, policy, standards, planning, and investment. Work with departments to use corporate approach.
Alberta	Not identified	Chief Information Officer	Office of the Chief Information Officer	Ministry of Innovation and Science	Deputy Minister	Provide leadership. Promote and facilitate strategies. Work closely with Council of departmental CIOs.
Saskatchewan	Deputy Ministers Steering Committee on Information Technology	Chief Information and Services Officer	Information Technology Office	Agency	Minister responsible for Information Technology	Establish and coordinate policies and programs to enhance electronic service delivery and e-commerce. Works with departments and agencies.
Manitoba	Non-existent	Chief Information Officer	Office of Information Technology	Department of Energy, Science and Technology	Deputy Minister	Develop strategy and architecture, as well as design infrastructure. Set standards and ensure security. Cultivate cooperation and coordination between departments and agencies.
Ontario	Information and Information Technology Directions Committee (Board Secretary is Chair and members are at Deputy Minister level.)	Corporate Chief Information Officer	Office of the Corporate Chief Information Officer	Management Board of Cabinet Secretariat	Secretary to Management Board of Cabinet	Lead and coordinate the IT function, including implementing IT strategy. Manage corporate IT infrastructure. Business Cluster CIO's report to both the Corporate CIO and to the Cluster Deputy Minister.
Quebec	Not identified	Under Secretary of Computer Networking and Information Resources	Under-Secretariat of Computer Networking and Information Resources	Treasury Council Secretariat	Treasury Council Secretary	Ensure optimal use of information technology by government. Collaborate with departments and agencies.
New Brunswick	Not identified	Chief Information Officer	Corporate Information Management Systems	Department of Supply and Services	Deputy Minister	Provide leadership, guidance, and a corporate focus. Also, manage services provided to departments such as data and voice networks, as well as data preparation and control.

Appendix C

ANALYSIS OF CHIEF INFORMATION OFFICER (CIO) ORGANIZATIONS BY JURISDICTION

(Based on Review of Internet Web Sites Maintained by Jurisdictions)

Jurisdiction	Strategic Planning or Steering Committee	CIO Title	CIO Unit	Location of CIO Unit	Report To	CIO Unit Role and Relation to Departments
Nova Scotia	Business and Technology Advisory Committee	Not identified	Corporate Strategies	Office of Economic Development (Merger of Technology and Science Secretariat with Department of Economic Development on March 11, 2002.)	Deputy Minister	Provide leadership and coordination in developing corporate strategies, policies and standards. Work closely and develop partnerships within provincial government.
Prince Edward Island	Not identified	Chief Information Officer	Information Technology Management Group	Department of the Provincial Treasury	Deputy Minister	Provide leadership, accountability and delivery of information technology support services to the public sector.
Newfoundland	Not identified	Director, Information Technology Management Division	Information Technology Management	Treasury Board Secretariat	Secretary to Treasury Board	Provide information technology services, including systems support to some departments and agencies, as well as advisory services to government in general and departments.
Yukon	Not identified	Director, Information & Communica-tions Technology	Information & Communica-tions Technology Division	Department of Highways and Public Works	Deputy Minister	Develop corporate strategies, procure technological solutions, and develop record management systems and procedures.
Northwest Territories	Informatics Policy Committee (Deputy Ministers)	Chief Information Officer	Chief Information Office	Treasury Board Management Secretariat	Treasury Board Secretary	Provide cross-government leadership and work closely with Deputy Ministers.
Nunavut	Not identified	Chief Information Officer	Information Management Branch	Department of Finance	Deputy Minister	Establish strategy, develop policy, set standards, and coordinate development.

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY

1.0 Background

Security over computer systems is a growing concern. Legislation increasingly requires organizations to protect the privacy of personal information, more and more of which is being collected in computer systems. At the same time, organizations see a continuing rise in security incidents. For example, news media periodically report that hackers deface Web pages and circulate computer viruses, and that thieves steal credit card numbers from computers. The main concerns about computer security are often categorized as maintaining the confidentiality, integrity, and availability of information or services.

Attacks on computers take a variety of forms. For example, computer penetration programs operate over the Internet or other computer networks to gain unauthorized control of a computer. Computer "denial of service" programs operate to shut down another computer or a service provided by that computer. Sniffer programs listen to computer network traffic to extract usernames and passwords. Viruses are programs designed to spread themselves by first infecting particular files on computer disks and then making copies of themselves. Viruses usually operate without the knowledge of the computer user and cause undesirable effects.

While organizations can protect themselves by maintaining their systems against known vulnerabilities, they are still exposed to unknown vulnerabilities. As a result, having good security measures in place will not guarantee prevention of computer security incidents. Therefore, it is important to be prepared and proactive about detecting and responding to such incidents when they do arise. Just as having sprinklers and fire drills as part of fire prevention, having a planned response to security incidents is part of effective computer security.

The Office of Information Technology (OIT) is responsible for ensuring the security of government systems, confidential information, and electronic transactions, and is headed by the Chief Information Officer (CIO) of the Province, who reports to the Deputy Minister of Energy, Science and Technology. OIT sets standards and best practices that it promotes throughout the government. In November 1999, the Information Protection Centre (IPC) was created as part of OIT. IPC ensures that "Government computer networks remain secure yet open, accessible and reliable."

Desktop, Telecommunications and Network Services (DTNS) is a branch of the Department of Transportation and Government Services. DTNS administers the contract with the service provider who manages the computers, printers and standard software used by Provincial personnel, as well as the computer servers that provide printing, e-mail, and other local area network services. This service provider also offers help desk support, as well as education and training services to Provincial personnel. This arrangement is referred to as the "managed environment."

Moreover, DTNS administers the contract with another service provider who supplies and manages the provincial data network linking departments, agencies and other operations. As well, DTNS administers the contract with a third service provider who supplies local and long-distance telephone services.

The Insurance & Risk Management Branch of the Department of Finance is responsible for the Risk Management Policy of the Province.

2.0 Audit Objective, Scope and Approach

The objective of our audit was to determine if the Province is capable of properly responding to computer security incidents at Departments.

Our examination included the computer environment managed by a service provider for Departments, as well as computer application servers managed by those Departments. Other computer operations of the Province were excluded.

Specifically, we examined the processes for:

1. Preparing to deter and handle computer security incidents.
2. Identifying whether or not an incident has occurred, and if one has occurred, determining the nature of the incident.
3. Containing the scope of an incident.
4. Eliminating the problem.
5. Restoring computer systems to fully operational status.
6. Following-up incidents to identify improvements to incident handling.

These processes and their accompanying actions are identified by various information technology security publications and organizations, such as the SANS Institute (SANS). SANS is a cooperative research and education organization through which system administrators, security professionals, and network administrators share information. Therefore, the Province's processes for managing computer security incidents were assessed against accepted good practices.

Our audit was conducted during the period September 2001 to February 2002, and included interviews of officials and examinations of policies, procedures and other documentation.

The Department response indicates a number of actions they have taken subsequent to our fieldwork.

We conducted our audit in accordance with the public sector value-for-money auditing standards recommended by the Canadian Institute of Chartered Accountants, and accordingly included such tests and other procedures, as we considered necessary in the circumstances.

3.0 Summary Conclusion

We concluded that based on a review of the above-noted processes, the Province is capable of properly responding to computer security incidents involving either the computer environment managed by a service provider for Departments or the computer application servers managed by those Departments.

However, we have identified opportunities for improving security procedures. A separate detailed report was provided to OIT, DTNS, and the Insurance & Risk Management Branch providing detailed recommendations.

We consider the following five areas to be of particular importance.

4.0 Findings and Recommendations

4.1 KNOWN SYSTEM VULNERABILITIES SHOULD BE PATCHED

Most computer system intrusions occur through known vulnerabilities. To prevent such intrusions, it is important to configure computer systems securely and keep current with security updates or "patches" provided by the system vendor.

Currently, the Province lacks the means to ensure that the managed environment service provider and Departments apply available security updates on a timely basis. IPC monitors vendor and security news services to find out about vulnerabilities and security updates. IPC advises the managed environment service provider and Departments about critical vulnerabilities and security updates for computer operating systems, basic application software and computer viruses. However, there is no mechanism to ensure that updates are applied.

For example, IPC reports that security-related updates are not always applied to network servers in the managed environment on a timely basis. Furthermore, Departments may not be aware of security updates for the non-basic application software installed on user computers and Department server computers. IPC does not track the non-basic application software installed on user and server computers. Nor does IPC monitor vendor and security news services regarding security updates for such software.

In addition, a significant number of computers (about 3,500) continue to use an operating system that does not have robust security features. Also, the software developer announced effective June 30, 2003 it will stop support of the operating system version used on another approximately 7,300 computers. If security concerns arise with unsupported software, it might not be possible to resolve them. For the fiscal year ended March 2003, the Province intends to replace about 1,200 out of 10,500 computers in the managed environment with new computers having a recent operating system version. The technological infrastructure plan has no timetable to upgrade or replace the remaining computers.

Consequently, there is an increased risk of successful attacks on the Province's computer systems.

In passing, we noted that the Province has not developed a strategic plan for information technology that aligns with the business objectives of the Province and is supported by a technological infrastructure plan.

We recommend implementing arrangements to ensure that security updates are applied on a timely basis to computers.

We recommend developing a technological infrastructure plan that specifies technology that is suitably matched with the strategic plan for information technology and deals with security concerns about using older computers and operating system software no longer supported by the developer.

4.2 A SECURITY AWARENESS AND EDUCATION PROGRAM SHOULD BE IMPLEMENTED

Briefings, orientation sessions, and information circulars are good ways to inform users about computer security and security incident procedures. For example, providing users with a list of common indicators helps them recognize a possible security incident when they see it. Also, developing and maintaining a Security Incident Web Page on an organization's Intranet helps users locate the computer incident handling team.

Currently, the Province lacks a process for uniformly informing its employees about computer security in general, as well as incident handling procedures and the contact process.

Some information on security has been distributed to employees of the Province. Also, some information is available on the Province's Intranet. The IPC web site, on the Province's Intranet, discusses the computer security incident process and reporting procedures. For example, a list of examples of security incidents is available. Also, a list of indicators of computer viruses is included in the Workstation section of OIT security policies. In addition, the web site indicates that employees are expected to report suspicious activity regarding computers. However, users may not visit the IPC Intranet site, or read the information available on the site.

Consequently, there is increased risk that users will not recognize security events or report them.

We recommend that a program be established for informing and educating users about computer security.

4.3 SECURITY RELEVANT ACTIVITIES ON COMPUTER SYSTEMS SHOULD BE LOGGED AND MONITORED

Security relevant activities on computer systems should be logged and monitored. The indicators of undetected incidents, such as failed login attempts, often are hidden in computer system log files. It is important to read log files. Software tools should be provided to automate log file analysis as much as possible.

The managed environment service provider activates security relevant logging only upon request. Also, IPC advises that security incidents indicate a need for training of staff members who administer the application servers in Departments.

OIT policies indicate that monitoring should be done. The managed environment service provider uses standardized computer hardware and manages it on a centralized basis. Such an approach facilitates logging and monitoring security relevant activities. However, the contract with the service provider does not specifically discuss training, auditing, logging and monitoring logs for security purposes.

In contrast, computer hardware is not standardized for Departmental servers. The lack of standardization impedes the implementation of logging and monitoring of security relevant activities. Moreover, there is no uniform training program for Department staff regarding such security procedures.

Consequently, the managed environment service provider and Departments are not monitoring computer systems in the most effective manner for security purposes.

Some of the tasks performed by these staff members, such as intrusion detection analysis, ideally should operate on a 24 hour, seven days a week basis.

We recommend developing a plan to ensure that computer system logging and monitoring of security relevant activities is performed appropriately. Such a plan should include having servers in Departments standardized to the extent practical to ensure efficient and effective system administration, including the logging and monitoring of security relevant activities. Also, the plan should include ensuring that adequate security related training is provided to Department staff members who administer their application servers.

We recommend that activities, such as intrusion detection analysis, be reviewed to determine if they should be conducted not only during regular business hours, but during off hours.

4.4 A RISK MANAGEMENT PLAN SHOULD BE IMPLEMENTED

A risk management plan should be implemented. This plan should include conducting risk assessments and developing disaster recovery/business continuity plans. It is prudent to perform a risk assessment to identify critical computing assets that warrant additional protection. Moreover, critical business systems may have redundant components and back-up sites as part of a disaster recovery/business continuity plan. An organization could take advantage of these redundant machines and networks to continue business processing, in the event that the regular system is compromised by a security incident.

The Risk Management Policy for the Province does not specifically require Departments to develop risk management plans, including risk assessments and disaster recovery/ business continuity plans.

IPC does vulnerability assessments of computers and participates in assessing security issues regarding computer systems under development, as well as researching security approaches for proposed computer systems. IPC advises that vulnerability assessments will be conducted at all Departments during the fiscal year ended March 31, 2003.

However, there are no specific requirements for Departments to assess the risks regarding computer systems and the information processed on the systems, including matters such as privacy. Also, there are no specific requirements to contact risk management personnel, legal counsel, or Departmental representatives appointed under information protection and privacy legislation.

Currently, the Province does not have a disaster recovery/business continuity plan in place. However, a working group has been established to deal with the issues involved in being able to continue business operations despite a disaster, including the recovery of computer systems. Risk management personnel for the Province are part of the working group. Yet, DTNS advises that it is not represented in the working group.

Consequently, there is increased risk that protective measures will not be applied in the most effective manner, because risk assessments are not conducted. In addition, there is increased risk of significant disruptions to operations of the Province because a disaster recovery/business continuity plan has not been developed.

We recommend that the Risk Management Policy include specific requirements for risk assessments to be performed as part of strategic and business planning, as well as disaster recovery/business continuity plans to be developed with the involvement of all relevant groups.

4.5 APPROPRIATE AUTHORITY SHOULD BE GRANTED TO THE SECURITY INCIDENT HANDLING TEAM

The incident handling team has to make decisions regarding computer systems whose security has been compromised. Senior management should understand and support the level of authority granted to an incident handling team to make critical decisions, including the authority to take servers offline and disconnect networks. This authority should be documented in the incident response plan.

A Treasury Board minute established IPC but does not indicate what authority IPC has regarding security incidents. The IPC incident response plan indicates that IPC has authority to make critical decisions, such as disconnecting computer servers and networks from the Internet. IPC officials indicate that the IT Director and Security Coordinator for a Department may be involved in a decision to disconnect a departmental server from the Internet.

As the Province develops more Internet based applications to provide services to the public, the situation of disconnecting employees or Department applications from the Internet may affect services to a much greater extent in the future.

Consequently, there is increased risk that the ability of incident handlers, such as IPC, to make critical decisions may be hampered if an authoritative body, like Treasury Board, does not clearly grant appropriate authority.

We recommend that the Province clearly grant appropriate authority to make critical decisions regarding the handling of computer security incidents.

OIT Comments

The Office of Information Technology (OIT) agrees with the majority of the findings within this report and fully supports the recommendations for a Government-wide education and awareness program. The business plan for such a program is currently under development within IPC.

Due to the nature of the organizational structure of Government, it should be noted that this report includes some recommendations that must be carried out by organizations other than OIT. Specifically, there are recommendations within the report that refer to Desktop, Telecommunication and Network Services, Departmental Information Technology branches, and the Insurance and Risk Management Branch. OIT fully supports these recommendations as they are based on industry best practices.

Department Comments

We have progressed in a number of areas. Our IPC has started work on a government-wide security education and awareness program. Also, since the former DTN&S group is part of Manitoba Information and Communications Technologies, we are able to move ahead on improvements to our ability to patch known vulnerabilities and protect against viruses and other network issues.