3 CENTRAL FINANCIAL MANAGEMENT SYSTEM/SAP

BACKGROUND

3.1 The Corporate Financial Management System (CFMS) is a composite collection of several management information systems that form the central core of the government's financial management system. The most significant component of CFMS is SAP R/3. It is an enterprise resource planning system (ERP) which contains a variety of functional modules. CFMS has a variety of feeder systems used by departments which pass data to SAP R/3 either electronically through interfaces or through manually-created journal entries.

3.2 SAP R/3 was implemented by the Department of Finance on April 1, 1997. It has now been in service for over six years. There have been major upgrades both to the software and to the hardware infrastructure. In addition, SAP has been rolled out to other broader public sector entities and will continue to be implemented in more of these entities over the next several years.

3.3 The Corporate Information Systems (CIS) division of the Department of Finance is responsible for the overall management, maintenance and support of SAP for core government as well as for certain public sector entities. The latter is achieved through service level agreements.

3.4 The SAP Project Office, created in 2002 as part of the Office of Economic Development, is responsible for the strategic deployment of SAP across the Provincial public sector.

RESULTS IN BRIEF

3.5 The following are our principal observations.

- The Corporate Information Systems division does not have a formal planning process. There is no strategic plan for the division. There are certain components of operational planning in place, however they are not integrated and do not address all areas of the division's responsibilities. Finance's Business Plan makes no mention of the CIS division as a core business area or in its listing of priorities.

- SAP security was last audited in 1998. Issues identified this year point to the need for a comprehensive security and control audit to be completed, particularly since there are plans to implement the human resources module and electronic payments to vendors. For example:

- There are no formally documented policies and standards for CFMS security or for the correction and transport system.

- There has been inappropriate deployment of powerful security access privileges and there is a need for stronger management and control of user logon accounts.

- There is no formal disaster recovery plan to guide recovery, and no business continuity plan to enable the continued provision of essential services, if a disaster or other significant interruption of computer services was to occur.

- There were significant departures from the described control practices in the correction and transport system.

■ Service level agreements in place to define roles, responsibilities and service levels between CIS and broader public sector entities have not been reviewed by legal counsel and certain additional important clauses need to be included.

AUDIT SCOPE

3.6 Due to the magnitude and complexities of CFMS/SAP, our examination has been planned as a multi-year project. This year we focused on the overall management and control framework, as well as the control practices in selected areas.

3.7 Our overall objectives of the assignment this year were to review the control practices in place surrounding SAP including:

- information technology planning
- information systems acquisition, development and maintenance
- computer operations and information systems support
- information technology security
- business continuity planning and information technology recovery

3.8 Specific detailed control objectives for each of these areas were derived from the Canadian Institute of Chartered Accountants' *Information Technology Control Guidelines* (ITCG). Further, the specific and detailed criteria we used to assess each objective were also derived from ITCG. These objectives and criteria were discussed with and agreed to by management.

PRINCIPAL FINDINGS

Planning

3.9 The Corporate Information Systems division is responsible for the overall management, maintenance and support of the SAP System. The division is essentially broken down into three operational areas - BASIS Support (including security), ABAP Programming and Functional Management. In the spring of 2003, the division was further expanded to include the HRMS Support Group. The division currently employs approximately 35 staff and the Director reports to the Controller of the Province.

3.10 In terms of services, the division not only manages and supports SAP R/3 for the core government but also, through a series of service level agreements (SLA's), provides similar management and support to the following broader public sector entities:

- 7 school boards
- 7 Regional Housing Authorities
- 6 Municipalities

3.11 These entities are running independent instances of SAP directly from the government's SAP servers and related infrastructure. There are also general plans for future support arrangements to be provided by the division through SLAs to the Nova Scotia Public Service Commission and the District Health Authorities.

3.12 Considering the recent and rapid growth of the CIS division's responsibility to multiple and independent clients over an expanding array of SAP application modules, we expected to find an extensive and formalized planning structure for the division. When we enquired about the nature and extent of planning, we found that there is no formalized planning for the division in terms of a strategic plan. Certain components of operational planning, are in place, however, they have not been integrated and do not address all areas of management's responsibilities. In addition, there are no divisional performance standards and measurable performance targets defined which could be used to report upon the performance results of the division.

3.13 The lack of formalized planning is of significant concern. The CIS division is responsible for managing, maintaining and supporting the primary financial management system of government and has had its responsibility extended to provide similar services and support to other, broader public sector entities. SAP is a highly technical and complex array of system and functional modules requiring a wide range of specialized technical skills. To continue managing in this very complex environment without a formalized planning process significantly increases the risk of inefficient operations, missed opportunities, decisions based upon incomplete information, inability to react on a timely basis to important issues and the inability to measure and report upon performance. The complexity also increases the need for well-defined control standards and practices.

Recommendation 3.1

We recommend that senior management institute a formalized planning process for the Corporate Information Systems division so as to establish a clear vision and direction as well as a formalized process to set out the necessary operational requirements for the delivery of services to its various clients.

Department of Finance Business Plan

3.14 The Corporate Information Systems division has significant management and support responsibilities not only to the Department but to the entire Provincial corporate entity. We reviewed Finance's 2003-2004 Business Plan. There is no mention of the CIS division in the 'Core Business Areas' or in the 'Priorities for 2003/04' sections of the plan.

Policies, Standards and Practices

3.15 We determined that there are few formalized policies and standards related to either the operational use of CFMS/SAP by general users, or internal policies and standards for the CIS division.

3.16 In particular, there are two areas where formally-defined policies and standards are most important and we have been informed that they are not in place.

- Security - SAP has a very complex security architecture and in such an environment a formal, implemented security policy would provide a framework to enhance the efficiency and effectiveness of managing the security function. Several of the matters discussed in other sections of this Report identify weaknesses in control that would probably not exist if strong and well-defined security practices were in place.

- Change control process - In SAP this process is called correction and transport. Although a system was described to us detailing the procedures to be followed when effecting system changes, our examination of a sample of such changes revealed that the system was not being followed. The specific results of this testing are covered in another section of this Report.

Recommendation 3.2

We recommend that priority be given to developing and implementing formal detailed policies, standards and practices for security as well as for correction and transport.

Recommendation 3.3

We recommend that management conduct a formal review of all Corporate Information Systems division operational responsibilities and determine the overall nature and extent of policies and standards that should be in place to promote a control conscious environment aligned with industry standard information technology control practices.

Need for a Detailed Security Audit

3.17 The security component of SAP is very complex and had not been audited since 1998. A new user in SAP has, by default, no access rights. Specific access rights are derived from the combination of profiles, authorization objects, authorizations and transaction codes assigned to each user. These assignments are based on the specific operational tasks required to carry out the user's responsibilities.

3.18 Our audit focused on a relatively high level examination of security. We looked for security policies and practices and we focused on the use of powerful security profiles and authorization objects. Due to resource limitations, we did not extend our coverage to a detailed assessment of segregation of duties.

3.19 We encountered situations that raise serious concerns as to whether security has been given an appropriate level of consideration in managing CFMS/SAP. These matters have been reported separately to management and are not detailed here due to the confidential nature.

3.20 Based upon the nature and significance of these security issues, we believe that government should commission a full and independent audit of all aspects of SAP security as deployed by the Province. Further, government should consider establishing a project to develop or otherwise acquire security 'best practices' in an SAP environment. This could become a very strong management tool in helping to ensure that appropriate controls are in place and effectively maintained.

3.21 The need for a security and control audit is urgent. Implementation processes are well underway for the human resource module as well as for electronic payments to vendors. Before either of these areas are formally implemented, there must be a fully established and extensive definition and deployment of appropriate security practices, including formalized, regular monitoring of compliance. Once e-business, including electronic funds transfer, and web access are in place the risks of unauthorized access to the system and the unauthorized transfer of funds increase significantly. Only a strong, well-managed security and control system can reduce these risks to an acceptable level.

Recommendation 3.4

We recommend that government commission a full and independent audit of SAP security and control as soon as possible.

Recommendation 3.5

Further, government should consider establishing a project to develop or otherwise acquire security and control 'best practices' in an SAP environment.

Inappropriate Use of Powerful Access Rights

3.22 Most computer application systems provide for the granting of powerful user access rights to all aspects of the systems. This is usually referred to as a 'Super User' and is intended to facilitate initial setup of a system as well as to act as an emergency user when significant unforeseen circumstances occur. Industry standards and practices strongly suggest that the granting of such powerful access rights be highly controlled. They should only be used for specific instances and in each case with the express permission of senior management.

3.23 The most powerful security profile available in SAP is called SAP_ALL. If a user is assigned this profile, the result is unrestricted access to all components of SAP. This means that a user having this profile can do absolutely anything in SAP ranging from system configuration settings, modification of program code and table contents, and user management – all the way down to detailed transaction levels in each of the functional modules such as general ledger and accounts payable.

3.24 With regards to SAP_ALL, SAP security documentation states specifically

> *"This profile contains all SAP authorizations, meaning that a user with this profile can perform all tasks in the SAP system. You should therefore not assign this authorization profile to any of your users. We recommend that you maintain only one user with this profile. You should keep the password of this user secret (store it in a safe) and only use it in emergencies."*

3.25 During the course of our examination we encountered a number of situations relative to the use of the SAP_ALL profile which represent significant control risks. These matters have been reported separately to management and are not discussed here due to the confidential nature.

3.26 In addition to 'super-user' security profiles such as SAP_ALL, there are also several powerful authorization objects that should be closely controlled. Our review of certain of these indicated that they have been deployed in the production environment and, as a result, indicated that they are not being closely controlled with due consideration of the risks.

Recommendation 3.6

We recommend that the SAP_ALL profile should not be assigned to any staff or user ID in the production environment including BASIS staff. As a maximum there should only be one user ID established with this profile and it should be highly controlled and used only for emergency purposes.

Recommendation 3.7

We recommend that management review the deployment of all powerful security profiles and authorization objects. This review should focus on the appropriateness of such deployments and examine the associated risks as well as the adequacy of the controls established to mitigate these risks.

Analysis of System Users

3.27 At the time of our audit there were approximately 1,090 registered system users for core government. Through the use of analytic system reports we were able to determine:

- 351 user IDs had not been used in more than 180 days (6 months);
- 82 user IDs have never been used;
- 54 users have multiple user IDs; and
- a few user IDs exist for former departmental or government employees who have transferred to other departments or terminated employment with the government.

Recommendation 3.8

We recommend that a formal security policy be established including a component that specifically requires the following:

- Once an ID goes 180 days without use it should be locked and the user contacted to determine if the ID is still required.
- There should be an annual renewal of all user IDs to pick up changes in user responsibilities, movement of users between departments and termination of users.

Access to Change Key Global Accounting Settings

3.28 As part of our review of security access we utilized certain system-generated analytic reports to determine how many users had update capabilities for key global accounting settings including the chart of accounts, accounting periods and company codes. We determined that there were:

- 269 users who could update the Chart of Accounts;
- 48 users who could update Accounting Periods; and
- 48 users who could update Company Codes.

3.29 Only a select few people, probably in Finance's Government Accounting division, or the CIS division for Company Codes, should have the ability to change these key settings.

3.30 We followed up with security and functional managers to determine why so many users would have the ability to update these key global accounting settings and found the following.

- Chart of Accounts - The security manager found that there had been an error dating back to system implementation in 1997 whereby 221 of the 269 users with this access should not have had it. This access was immediately removed from these 221 users. The reasons for the remaining 48 users to have this access have not been reviewed.

- Accounting periods - Functional managers selected one of these users and tested the access capabilities and determined that, although the user had the system authorization, the user did not have the additional transaction code necessary to perform this task and therefore cannot actually update. However, only one user was examined and the other 47 have not been checked to determine if the same applies to them.

- Company codes - None of these have been checked to determine if the same scenario applies.

3.31 Management has indicated that it plans to create a special security role for government accounting which will contain these access rights and that any requests for such rights will require the approval of the Director of Government Accounting.

Recommendation 3.9

We recommend that all users listed as having the capability of updating key global accounting settings be examined to determine why they need these capabilities, and to assess the associated risks.

Use of Roles for Access Security

3.32 The SAP security architecture provides for the optional use of 'roles' as a means of creating and maintaining user access rights. Through the use of defined roles, security administration becomes more efficient and provides better consistency over the assignment of users' access rights. It also provides a framework to more easily establish and maintain an appropriate segregation of duties.

3.33 Roles are collections of authorizations and transactions that are executable by any user who is assigned that role. Multiple roles can also be assigned. An example of this role-based approach to security would be where the specific access requirements for a job function are defined, such as an accounts payable clerk. That role could then be universally applied to all accounts payable clerks across government with a limitation specified for them to perform the role in only their home departments.

3.34 We determined that the current approach to implementing security by the Corporate Information Systems division is not role-based. The current approach has evolved from the original implementation of SAP in 1997, when role-based security was not available. The functions of each individual SAP user were identified and the required authorizations were assigned to each. This made for a very complex and lengthy process for creating and maintaining system users.

3.35 We have been informed that management is now considering a conversion to the role-based approach, however, there are organizational challenges that need to be identified and addressed before this can be done.

Recommendation 3.10

We recommend that management make a determination of the issues and challenges in converting to a role-based approach to implementation of access security and develop a detailed transition plan for the conversion.

Disaster Recovery Plans

3.36 The overall purpose of a disaster recovery plan is to provide for an orderly and timely restoration of services in the event of an unexpected interruption through the failure of one or more key infrastructure components. Given the complexities and interdependencies of today's information technology infrastructures, the preparation of a disaster recovery plan represents a major task requiring the full support of senior management to commit qualified staff resources and to assign a high enough priority so that the plan will be completed in a thorough and timely fashion. Implementation of the plan may also require a commitment of resources such as redundancy of hardware or provision of an alternate site. There is also formal commitment required to ensure that the plan is tested on a periodic basis and that appropriate mechanisms are established to keep it up to date.

3.37 By virtue of overall responsibilities for the management, maintenance and support of the CFMS/SAP infrastructure and services, the Corporate Information Systems division is specifically responsible for the preparation and testing of appropriate and thorough disaster recovery plans for the CFMS/SAP infrastructure.

3.38 We understand that when the SAP servers and related infrastructure were physically housed in the Provincial Building, there was a disaster recovery plan in place. However, effective July 2002, the SAP servers and related infrastructure components were moved to the EDS Data Centre on Young St. in Halifax. Later, in 2002 there was a major change to the infrastructure where a completely different manufacturer's product was installed.

3.39 Upon the move to the EDS facility, the former disaster recovery plan became invalidated due to the significance of the changes. Although a new plan should have been completed to coincide with the move to the EDS facility, this was not done and there is currently no disaster recovery plan to be enacted in the event of failure.

3.40 We understand and appreciate that the CIS division has several significant initiatives underway. However, the requirement for a disaster recovery plan should receive the appropriate level of support and commitment from senior management, since the Province has now gone more than one year without such a plan.

3.41 A recent incident in the building which houses the EDS Data Centre is an example of a situation that could have caused problems. In spring 2003, it was publicly revealed that the building had a problem with mould in the air ventilation system. Although the mould was somewhat toxic, it was removed without shutting down the building. However, had it been a more toxic variety of mould, occupational health and safety regulations could have resulted in the building being closed for a prolonged period. Had this happened, the SAP system would have been shut down and unavailable for an undetermined period. The CIS Division would not have had any plans or arrangements in place to deal with and provide for the orderly resumption of service. The result could have been a prolonged shutdown of the government's financial management system, as well those of the public sector entities supported by the Province.

Recommendation 3.11

We recommend that senior management establish and test a disaster recovery plan as soon as possible.

Recommendation 3.12

We recommend that the SAP Projects Office should ensure that the standard project implementation methodology includes the evaluation of the disaster recovery plan against the business requirements. This evaluation will feed into the update of the business owners' existing Business Continuity Plan.

Business Continuity Plans

3.42 As there is a need for a disaster recovery plan, there is also a corresponding and significant need for business continuity plans. These latter plans are required to identify acceptable levels of services that need to be provided in case of an interruption of service. One potential cause of the interruption of service may be inability to access computer systems.

3.43 The primary responsibility for business continuity planning is not with the Corporate Information Systems division. It is the responsibility of the business owners' of a service to ensure there are business continuity plans in place, regardless of the cause of the interruption of service. There is a corporate responsibility to recognize the importance of business continuity plans and to ensure they are a priority. There was a recommendation to this effect as a result of the Y2K problem.

3.44 Accordingly, this is a matter that should be addressed by the Deputy Ministers' Forum and subsequently Cabinet.

Recommendation 3.13

We recommend the establishment of a policy requiring all departments to have an appropriate business continuity plan, and that this plan be kept up-to-date on an ongoing basis. Further, we recommend the establishment of an initiative to undertake the development and implementation of a corporate business continuity planning process.

Recommendation 3.14

We recommend that in conjunction with the development of a corporate business continuity planning process, that the Business and Technology Advisory Committee (BTAC) should also examine the needs for a corporate disaster recovery planning process, as it relates to the provision of computer services.

Recommendation 3.15

We recommend that the SAP Projects Office should ensure that the standard project implementation methodology should include updating the business continuity plan to reflect the new system.

Service Level Agreements

3.45 The Corporate Information Systems division has entered into formal arrangements with certain broader public sector entities to provide the infrastructure for independent instances of SAP as well as a variety (depending on individual entity needs) of system management and support services. The CIS division charges a fee for these services and has in place a separate service level agreement (SLA) with each of these entities that outlines roles, responsibilities and service levels. All of these agreements are drawn from the same basic template but it is unclear as to whether there has been a review of the agreements from a legal perspective, to ensure that the government is sufficiently and appropriately protected.

3.46 Agreements have been implemented for the following:

- 7 School Boards;
- 7 Regional Housing Authorities; and
- 6 Municipalities

3.47 These entities are running independent instances of SAP directly from the government's SAP servers and related infrastructure. There are also general plans for future support arrangements to be provided by the division through SLAs to the Nova Scotia Public Service Commission and the District Health Authorities.

3.48 We determined that there is no specific mention in the SLAs of each party's responsibility for disaster recovery and business continuity planning. These are important clauses that should have been included.

3.49 We also determined that there is no provision in the agreements for an independent service auditor review and reporting on controls. Such a report would provide assurances to the governing bodies and management of entities using the central SAP infrastructure and services provided by CIS, that sufficient and appropriate controls are in place to provide a secure processing environment. As well, it is likely that the financial statement auditors of the various school boards, municipalities and other entities which are parties to these service level agreements will be approaching the CIS division with information requests concerning the controls in place over the SAP infrastructure.

3.50 As a final matter, we also noted that, although the SLA for the municipalities has been in use for several months, the agreement has not yet been signed. We understood there were plans to have it signed in September 2003. In future, such services should not be provided until the agreements are formally executed.

Recommendation 3.16

We recommend that the current service level agreements should be reviewed by legal counsel.

Recommendation 3.17

We recommend that the agreements contain clauses to specifically address each party's responsibility for disaster recovery and business continuity planning.

Recommendation 3.18

We recommend that government address the need for an annual service auditor review and reporting on the controls surrounding the SAP infrastructure and related Corporate Information Systems services.

Correction and Transport

3.51 Once a computer system is installed, it requires ongoing maintenance to correct discovered errors, to meet changed circumstances or to provide enhancements to meet evolving user needs. Such changes must, of course, be carefully controlled and in the SAP R/3 environment control is achieved through the 'correction and transport system'. This system is also used to make changes to system tables such as the currency exchange table which must be changed on a daily basis. As well, this system moves changes from the SAP development environment to the quality assurance environment and finally into the production environment. The correction and transport system tracks all changes by automatically assigning a control number anytime that any element of SAP is changed. Security access controls should be deployed in a manner to ensure that only key BASIS staff can promote changes through the hierarchy from development to production.

3.52 Our review of the Corporate Information Systems division use of the correction and transport system involved obtaining a description of the system. We then selected a sample of items from the logs of the transport system. We compared the documentation of each sample item to the described system.

3.53 We found that there was inadequate documentation regarding the policies, standards, procedures and practices of the correction and transport system in the CIS division. Our description of the system was obtained verbally through interviews with CIS management and staff, and was supplemented by a listing of procedures conveyed to CIS staff by management.

3.54 When we examined our sample we found the following:

- no two of the sample items were processed in the same way by the staff of CIS;
- most deviated significantly in one or more ways from the described system;
- none of the samples followed the described procedure completely;
- several of the samples had no documentation at all and for most of the rest the quantity and quality of documentation was inadequate; and
- in most cases there was no evidence of approvals.

3.55 A formalized policy and standard practices in this area would help to minimize the risks of unauthorized and/or untested changes being made to systems. Documented and enforced procedures help to provide assurances that controls are in place, encourage compliance and simplify management of change.

3.56 As a final matter, the government operates a problem tracking software called 'Remedy'. This allows computer users who have a problem to contact a 'help desk'. Staff at this desk assign a unique ID number to the complaint and refer it to the appropriate staff for action. The ID numbers are tracked by the Remedy system. Managers can see who has outstanding items and the functional staff can see which task they need to work on. Those staff who prepared adequate documentation did so using the documentation functionality of the Remedy system.

Recommendation 3.19

We recommend that appropriate policies and procedures for using the SAP correction and transport system be designed, documented and implemented.

Recommendation 3.20

We recommend that use of the 'Remedy' system, or an acceptable alternative determined by management, be considered to manage the work flow of the SAP correction and transport system.

CONCLUDING REMARKS

3.57 The Corporate Information Systems division has very significant responsibilities in regards to the management, maintenance and support of SAP which provides the government's core financial management systems. Such responsibilities have been extended to provide similar service functions to several other public sector entities, which are running independent instances of SAP on the SAP infrastructure managed by CIS.

3.58 Government should be concerned with the lack of formalized planning, the absence of policies and standards and the prolonged use of inappropriate security practices within the CIS division.

3.59 Plans are already in process to implement further modules of SAP, including human resources and business warehouse. As well, there is an additional project underway to implement electronic payments to vendors. Concerns identified to date should be fully addressed before such projects are finalized.

3.60 Government needs to take significant measures to ensure that appropriate planning processes are put in place and that detailed policies, standards and controls are developed, particularly in the area of security.

Exhibit 3.1

Nova Scotia Public Sector Deployment of SAP - April 2003

Modules/Entities	Core Government	School Boards	Municipalities	Regional Housing Authorities	District Health Authorities
Financials	I	I	I	X	P
Human Resources	U	U	I	I	P
Materials Management	I	I	I	X	P
Plant Maintenance	I	P	C	X	P
Internet Portals	U	C	C	X	C
Business Warehouse	C	I	X	X	P
Customer Care Service	C	X	U	X	X

I = Implemented
U= Projects Underway
P= Planning Completed
C= Under Consideration
X= No Plan to Implement