Science and Engineering Research Canada

NSERC
CRSNG

Audit of the electronic Common Information Management System (eCIMS) Development Project

December 2004

Natural Sciences and Engineering Research Council of Canada
Conseil de recherches en sciences naturelles et en génie du Canada

Canada

Table of Contents

Executive Summary

Detailed Report

Executive Summary

Introduction

The audit of the electronic Common Information Management System (eCIMS) development project is included in the Audit Plans for 2004-05 of both the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council of Canada (SSHRC). Accordingly, the audit has been conducted jointly by the two Councils.

The Councils' Corporate Risk Profiles identified outdated processes for recorded information, particularly in terms of electronic information life-cycle management, as a key risk to their capacity to manage and report accurate and complete Council information to various stakeholders. The Profiles also recognized the related risk of corporate memory loss. The eCIMS project was established to mitigate these risks.

The eCIMS is part of the Councils' initiative to improve the management controls over recorded information, both electronic and paper-based. It is intended to help by:

- automating many of the processes and procedures used in the life-cycle management of recorded information, and
- providing sufficient comprehensive control over the organizations' various record collections.

The eCIMS development has reached a critical phase. The project has scheduled a four-month limited implementation pilot starting on December 1, 2004 and ending on March 31, 2005. The purpose of the pilot is to stress test the system and to create and revise training, maintenance, and support procedures before the system is rolled out to the two Councils. The Councils will use the results of the pilot to determine whether to proceed with the system.

Audit Objective, Scope, and Timing

The audit provides an independent and objective assessment of the management control framework established to ensure that the eCIMS development project will succeed. The control framework is composed of the guidance, procedures, and activities that management establishes to ensure that objectives are achieved.

The audit focused on the key risks inherent in the project. The auditor's assessment of these risks, the related criteria used to exercise the audit objective, and the audit methodology and approach are detailed at Appendices A, B, and C respectively.

The audit was conducted in November 2004 and examined the eCIMS development project's achievements to date and plans for the future.

Overall Audit Assessment

***Auditor's Statement of Assurance**: The auditor has performed the work required to provide an independent and objective assessment of the management control framework established to ensure that the eCIMS development project will succeed.*

The eCIMS project has taken a number of very important steps in the development of an information management (IM) system for the Councils. It has spelled out a Business Case for raising the priority of the system development and garnered the Management Committees' support for additional resources to address the priority; started the process of acquiring the requisite expertise; established a Project Plan and a Limited Implementation Pilot Project Plan, setting out a preliminary threat and risk assessment, development activities, roles and responsibilities, deliverables, timelines, resourcing, and reporting schedules; commenced project reporting; obtained an Information Systems Division (ISD) resource for technical support; created a Steering Committee to guide the project; initiated a user group for the pilot; and drafted a Communications Plan. The project has also adopted two proven techniques to reduce the risks inherent in system development: It has acquired a commercial off-the-shelf (COTS) system and is phasing it in using a limited implementation pilot.

To ensure their effectiveness, these actions need to be supplemented with:

- **An appropriate governance structure and accountability process that place the Councils' senior management in charge of monitoring the project's progress and use of resources and leading the change management strategy that is critical to the new system's acceptance by users.**

  Senior management has long recognized the importance of an effective information management system to the work of the Councils. The sense of urgency is demonstrated by the Councils' Management Committees' identification of IM as a priority in the corporate risk analyses and the conduct of this audit of the eCIMS development. Furthermore, the Councils are currently conducting a complementary audit of the information technology function. While senior management has participated in the project since the beginning, it has not played a governance role in approving and monitoring progress against the project plan. It has neither asked for nor received proper accountability reporting on the delivery of the commitments made for the IM system and the use of the resources allocated to it. Senior management has not led the development of the change management strategy and plan required to overcome resistance to the new system and to ensure its effective use throughout the Councils.

- **Improved estimation, reporting, and monitoring of the costs and timelines of the system development.**

  While the project has undertaken adequate action to mitigate many of the risks inherent in the eCIMS development, the measures to manage the costs and the timeliness of the project need to be improved. The risks of cost and time overruns for the eCIMS project are heightened by the two-year history of the development and the relatively recent appointment of the current project manager in December 2003, creation of the eCIMS Project Plan in July and the Limited Implementation Pilot Project Plan in November 2004, and ongoing resourcing of the project. There has been no systematic estimation of the projected total costs and time for the development, and monitoring and reporting of the actual costs and time and any variance to date to the Management Committees as part of their decision-making process.

- **Increased user representation in all phases of the project, including the limited implementation pilot.**

  The project has reduced the programming risks in system development by deciding to install the COTS system as is, without any modifications. COTS systems, however, need to be configured or customized for the organization and, therefore, carry their own risks, which must be managed as rigorously as those of an in-house development. One of these risks is that the system's implementation will be effected without appropriate user participation. If users are not involved in the project, the system that is implemented may not meet their needs; users may abandon the project and the system that it delivers; the system's controls may not ensure the confidentiality, integrity, and availability of the information it produces; and business processes may not be changed appropriately. The challenges are enhanced by the existence of the two sets of users that constitute NSERC and SSHRC.

  We appreciate that the project has intentionally restricted the pilot to the Administration Division of the Common Administrative Services Directorate (CASD) in order to keep the test of the system manageable and efficient. On the other hand, the pilot's limited scope within a single site poses the risk that the user community's perspective, especially of those in the program areas, may not be completely and accurately represented. Furthermore, the criteria developed to assess the results of the pilot may not reflect the user community as a whole.

  We understand that, to address these risks, the project is considering a phased approach that will ensure appropriate user representation through the course of the development.

- **Use of an appropriate system development methodology (SDM) for all phases of the project, including the limited implementation pilot.**

  As noted, the eCIMS project is using two proven techniques to reduce the risk of the development: a commercial off-the-shelf (COTS) system and a limited implementation pilot. To ensure their effectiveness, however, these techniques need to be managed through an appropriate system development methodology (SDM). COTS systems carry risks that must be managed as rigorously as those of an in-house development. Customization of COTS systems is a part of system configuration, integration, and installation and, as such, can become invisible if not adequately documented. COTS systems' configuration and integration activities can require as much attention to code and language as traditional development activities.

In addition, the development of appropriate criteria for assessing the limited implementation pilot, the tests to be conducted, the expected results, and the methodology to collect and analyze the related data must be completed properly before the start of the pilot.

Detailed Report

Background on Information Management (IM)

Treasury Board Policy

The Treasury Board of Canada's (TB) Policy on the Management of Government Information, effective May 2003, defines IM as "a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal and/or long-term preservation."

Among other things, the Policy obliges federal government institutions to:

- "manage information to facilitate equality of access and promote public trust, optimize information sharing and re-use, and reduce duplication, in accordance with legal and policy obligations,
- use electronic systems as the preferred means of creating, using, and managing information,
- protect essential records to ensure the continuity of key services and business operations,
- preserve information of enduring value to the Government of Canada and to Canadians, and
- dispose of information no longer required for operational purposes in a timely fashion."

Corporate Risk Assessments

NSERC's Corporate Risk Profile for 2004-2005 identifies "outdated processes for recorded information particularly in terms of electronic information life-cycle management" as a key risk to its "capacity to manage and report accurate and complete Council information to various stakeholders."

SSHRC's Corporate Risk Profile, October 2003, also identifies information management as one of the five major risk areas that the Council has to manage. The Profile observes that "SSHRC relies on a single, comprehensive data base for the management of all its grants and scholarship competitions and for reporting on outcomes and expenditures. While its records on individual files are extremely well maintained, the tradition of an oral culture prevails for sharing information." The Profile states that the related risks include corporate memory loss.

The eCIMS development project was created to mitigate these risks.

Risk-Based Annual Audit Plans

Consequently, the NSERC and SSHRC Risk-Based Audit Plans for 2004-05, which have been approved by their respective Councils, schedule information technology (IT), information management (IM), and electronic service delivery (ESD) for auditing during this year.

For the last three years, NSERC has undertaken annual audits of its ESD project called eBusiness Initiative, which is bringing key NSERC services on-line. NSERC will be auditing the project again this year. In addition, NSERC and SSHRC are currently conducting a joint audit to assess the effectiveness and efficiency of the IT function. The audit of the eCIMS development project addresses a core component of both IM and ESD.

Audit of the Recorded Information Management Function, August 2001

The risks associated with NSERC's and SSHRC's recorded information have long been recognized. In 2001, the Councils contracted Nashel Management Inc. to conduct an audit of the Recorded Information Management Function. Nashel's audit report, August 2001, identified three major needs:

- To improve the management control framework for recorded information, both electronic and paper-based.
- To exercise sufficient comprehensive control over the organizations' various record collections.
- To improve the technology and the handling, storage, and disposal procedures used in the life-cycle management of recorded information.

Information Management Strategic Plan, October 2002

In 2002, the Administration Division, CASD, created an IM Strategic Plan which identified the following to be undertaken to establish a new IM business model: developments of the IM function's mandate and vision, IM policy, IM staff profiles, communication and promotion plan, and technical solutions. The development of an IM technology infrastructure was an integral part of the business model. We understand that the Plan was approved by the Councils' Management Committees in November 2002.

Follow-up of the Audit of Recorded Information, November 2002

In 2002, the NSERC Senior Internal Auditor undertook a Follow-up of the Audit of Recorded Information to assess the progress made by management in addressing the issues raised by Nashel. The auditor's report noted that, while the IM Strategic Plan furnished an overview of the IM business model, it was not the detailed action plan that was required for a successful implementation. The report advised management to monitor closely the development of the detailed action plan and the progress made in implementing it.

The report also identified the greatest risk to NSERC and SSHRC as the implementation of a technological solution that would not meet their requirements. It recommended that a system under development audit of the technology project be performed in 2004-2005, to assess whether appropriate structures and controls have been established to ensure the success of the project.

Organizational Redesign Project, March 2004

In 2003, the Common Administrative Services Directorate (CASD) initiated the Organizational Redesign Project with a view to developing a model for a responsive, effective, and efficient delivery of information management (IM) services. The project report "Building an Information Management Service," issued in March 2004, set out a target model for IM services; analyzed the gaps between the model and the current organization, processes, and practices at the Councils; and recommended an implementation strategy for moving forward.

The gaps identified in the report included deficiencies in the IM technology infrastructure and related content and life-cycle management processes for recorded information. The report concluded that the implementation of the eCIMS along with supporting tools and training was critical to the success of the proposed IM service model.

eCIMS Business Case, April 2004

On April 8, 2004, the Chief of Information Management (CIM) presented the eCIMS Business Case to the NSERC Operations Committee, which has the mandate "to make recommendations to Management on corporate priorities taking into consideration the availability of resources."

The Business Case requested that the project be reassigned as soon as possible from "should" to "must" status in the schedule of project priorities, in order to ensure that adequate resources are allocated to complete the system in time for the rollout of the eBusiness Initiative projects. The eBusiness projects include internet-enabled tools that are bringing key NSERC services on-line. The eCIMS will process eBusiness information products in addition to other documentation.

The Operations Committee endorsed raising the priority of the eCIMS project to the highest level. We understand that the NSERC Management Committee approved the Business Case in April 2004.

The eCIMS Development Project

The Chief of Information Management (CIM), within the Administration Division, Common Administrative Services Directorate (CASD), is the Project Manager for the eCIMS development. The Director of Administration is the Project Authority, and the Director General of CASD is the Project Champion.

According to the eCIMS Business Case, the eCIMS development project is tasked with developing and implementing an electronic information management (IM) solution for use by NSERC and SSHRC. As explained in the Business Case, the eCIMS "is the result of a number of business drivers identified within the last few years as a result of internal audits, e-business initiatives, and demands from Council partners and clients. It is also in response to the policy direction given by Treasury Board of Canada in its Policy on the Management of Government Information issued in 2003."

The eCIMS is part of the Councils' initiative to improve the management controls over recorded information, both electronic and paper-based. It is intended to help by:

- automating many of the processes and procedures used in the life-cycle management of recorded information, and
- providing sufficient comprehensive control over the organizations' various record collections.

For life-cycle management of recorded information, the Councils procured and implemented the iRIMS system in 2001-02. iRIMS supports the creation, retention, and disposition of all records and information holdings, in paper and electronic format. It has since been renamed Livelink Records Server by Open Text Corporation, the company that has acquired it.

In 2003-04, to provide sufficient comprehensive control over their various record collections, the Councils purchased the Livelink Web-based Suite for document management. The Suite provides a repository for storing and organizing electronic documents. This system integrates with the iRIMS/Livelink Records Server records management system.

Estimated Costs of the eCIMS Project, November 2004

An estimate, based on information supplied by the project, yields the following costs of the eCIMS project to date. These costs relate to both Councils, with NSERC and SSHRC bearing 70% and 30% of the costs respectively.

Year of Cost	**Event**	**Estimated Costs April 2001 to November 2004** **$**
2001-02	Acquisition of an iRIMS Records Management System	50,000
	Personnel costs (Business Analyst) – based on estimate of time spent on iRIMS	10,000
2002-03	Acquisition of the Livelink Document Management System	150,715
	Replacement of iRIMS by the Livelink Records Management System	0
	Personnel costs (IM Business Analyst and consultant) – based on estimate of time spent on the eCIMS	45,000
2003-04	Purchase of server for eCIMS	48,500
	Personnel costs (IM Business Analyst and consultant) – based on estimate of time spent on the eCIMS	42,500
2004-05	Planned Costs • Learning tools (eCIMS manual, user manual, quick reference, course): $85K • Open Text professional services: $40K • Email and MS Suite integration: $35K • Training for Certified Livelink Administrator: $12.5K • Translation: $20K • Project reserve: $7.5K	200,000
	Personnel (25% CIM) – based on estimate of time spent on the eCIMS	20,000
	Total	**$566,715**

Detailed Audit Observations, Discussions, and Recommendations

As elaborated in the discussions below, the eCIMS project has taken a number of very important steps in the development of an information management (IM) system for the Councils. To ensure their effectiveness, these actions need to be supplemented with:

1. An appropriate governance structure and accountability process that place the Councils' senior management in charge of monitoring the project's progress and use of resources and leading the change management strategy that is critical to the new system's acceptance.

Observation

Senior management has long recognized the importance of an effective information management system to the work of the Councils. This urgency is demonstrated by the Councils' Management Committees' identification of IM as a priority in the corporate risk analyses and the conduct of this audit of the eCIMS project. Furthermore, the Councils are currently conducting a complementary audit of the information technology function.

While senior management has participated in the eCIMS project since its beginning, it has not played a governance role in approving and monitoring progress against the project plan. It has neither asked for nor received proper accountability reporting on the delivery of the commitments made for the IM system and the use of the resources allocated to it. Senior management has not led the development of the change management strategy and plan required to overcome resistance to the new system and to ensure its effective use throughout the Councils.

Discussion

Governance and Accountability

According to the Office of the Auditor General's (OAG) 2000 Report on Information Technology: Acquisition of Goods and Services, "Senior sponsorship and appropriate governance are key ingredients in successfully implementing large IT projects." In its Report on Information Technology – Government On-Line, November 2003, the OAG states that "governance consists of the leadership and organizational structures and processes to help ensure that the government achieves its vision…." In other words, governance is setting and giving strategic direction along with the related authority and responsibility, and requiring accountability for performance.

In its paper, Modernizing Accountability Practices in the Public Sector, the Treasury Board of Canada Secretariat (TBS) defines accountability as "a relationship based on the obligation to demonstrate and take responsibility for performance in light of agreed expectations."

While there is no one optimum governance model for everyone, all governance structures should distinguish between giving direction and supervising on the one hand and managing and doing the work on the other.

The eCIMS Project Plan, produced by the Chief of Information Management (CIM) and approved by the Director General of CASD and the Directors of ISD and Administration on July 14, 2004, proposes a governance structure of an eCIMS Steering Committee comprising the DG of CASD, the Directors of ISD and Administration, CIM, and a representative from the NSERC eBusiness Steering Committee and the SSHRC Electronic Services Delivery (ESD) Steering Committee respectively. It is our opinion that, while it has an important role to play in guiding the progress of the project, the eCIMS Steering Committee is neither structured nor positioned to provide corporate governance.

The NSERC and SSHRC Management Committees have participated in some of the major milestones of the eCIMS development since its inception. They have approved the *Information Management Strategic Plan, October 2002; Organizational Redesign Project, March 2004;* and the *eCIMS Business Case, April 2004.* As part of their approvals, the Management Committees have committed human and financial resources requested over time by the project, most recently the additional resources requested by the eCIMS Business Case in April 2004.

The eCIMS Project Plan furnished the following updates on the scope and approach of the system development:

- Livelink will not be rolled out to the Councils in the first year, 2004-05, but its implementation will be phased over two years.
- In year one, a limited implementation pilot of the system will be carried out from December 2004 to March 2005 within the Administration Division of CASD. The purpose of this pilot is to exercise the system's configuration in a live environment; complete the Threat and Risk Assessment and the Privacy Impact Assessment for the new system; establish a Service Level Agreement with the Information Systems Division (ISD) for the operation and technical support of the eCIMS; and evaluate the system with Administration users.
- The results of the evaluation will be presented to management for its decision on the next steps.

The Plan details the project's objectives, scope, methodology; a work break-down structure that lists the project activities, outputs, and resources; a governance structure for the development; a preliminary threat and risk assessment and mitigating actions for the system; roles and responsibilities for CIM and ISD; an estimate of time and resource usage in 2004-05; a Gantt chart illustrating project dependencies and milestones and related approval points; and monitoring and control activities.

While the Management Committees have approved and monitored the progress of the eCIMS as part of the design and implementation of the new IM business model, they have not played a governance role in approving and monitoring progress against the project plan. They have neither asked for nor received proper accountability reporting on the delivery of the commitments made for the IM system and on the use of the resources allocated to it.

Change Management

The eCIMS Business Case, April 2004, highlighted the risk to the project related to resistance to change: "The project requires that…employees learn the system and use it assiduously in order to make it their sole information repository. This will mean continuous learning for employees and coaching by supervisors. This information management culture change will take time to fully implement among all Council employees. It will require the cooperation of supervisors and management to ensure that Council employees transit to the new information management culture by using the electronic storage tool….The practice of creating and sharing information from its inception is foreign to Council staff, as it is to all government employees." The project is developing a Communications Plan to disseminate information on the development and the system across the Councils.

While it recognizes the challenge, senior management has not led the development of the change management strategy and plan required to overcome resistance to the new system and to ensure its effective use throughout the Councils. An effective change management strategy is an important consideration in management's decisions on the new system and should encompass communicating a sense of urgency for the project and the system throughout the Councils; creating a cross-functional leadership team to guide and sponsor the eCIMS; developing a clear vision for the eCIMS; communicating this vision frequently throughout the Councils; empowering employees to work towards the vision by removing barriers to action; achieving and recognizing short-term successes to demonstrate that the change is working; consolidating the successes to keep the project going; and anchoring or embedding the change within the organizational culture.

Recommendation:

1. The Councils' Management Committees should establish a joint NSERC and SSHRC eCIMS Governance Committee, comprising senior management, to provide strategic direction and oversight for the eCIMS development by:
   a. Demanding and receiving proper accountability reporting on the delivery of the eCIMS commitments and the use of resources allocated to them.
   b. Taking the lead in the development and implementation of a change management strategy for the eCIMS.
   c. Reporting periodically on the project's progress to the Management Committees.

2. Improved estimation, reporting, and monitoring of the costs and timelines of the system development.

Observation

While the project has undertaken adequate action to mitigate many of the risks inherent in the eCIMS development, the measures to manage the costs and the timeliness of the project need to be improved. The risks of cost and time overruns for the eCIMS project are heightened by the two-year history of the development and the relatively recent appointment of the current Project Manager in December 2003, creation of the eCIMS Project Plan in July and the Limited Implementation Pilot Project Plan in November 2004, and ongoing resourcing of the project. There has been no systematic estimation of the projected total costs and time for the development, and monitoring and reporting of the actual costs and time and any variance to date to the Management Committees as part of their decision-making process.

Discussion

As noted by the OAG's Report on Systems under Development: Managing the Risks, "it is imperative that the risks be identified, evaluated and effectively managed." Like most system developments, the eCIMS development faces risks that are related to the management of the project. These risks encompass:

- Improper scope. The system may provide insufficient or unneeded functionality to the organization.
- Unsatisfied user needs. The system that is developed may not meet the users' needs.
- Cost and time overruns. The system may be implemented late and at a greater cost than expected.

Improper Scope

In 2002, the Follow-up of the Audit of Recorded Information identified the greatest risk to NSERC and SSHRC as the implementation of a technological solution that would not meet their requirements. The project intends to use a limited implementation pilot to help management determine whether the technology meets the Councils' needs. Such a phased approach is considered a good practice for limiting the risks of system development.

The Project Plan, July 2004, recognized the risk posed to the development by the lack of appropriate staff resources. It warned that, if the resources could not be secured, the project would have to be scaled back and done over a longer term. The project has since obtained the additional funding for the personnel and professional expertise it deems necessary for the development.

Unsatisfied User Needs

The eCIMS development also faces the risk of unsatisfied user needs. To minimize the impact to the user of the move over to the new system and to maintain a link between legacy (hardcopy) and electronic information, the project has adopted the filing structure currently used in the Councils. This structure has evolved over the years in response to user requests. The continued use of the structure should ensure that users will be able to find legacy (hardcopy) documents and files and have these documents managed through their life-cycle along with electronic documents. The limited implementation pilot also will help in addressing some of the risks, although its impact will be reduced by its limited functionality and use by only the Administration Division of CASD. User representation in the project will be discussed in detail in the next section of the report.

Cost and Time Overruns

There has been no systematic estimation of the entire project's total costs and time schedule, and no monitoring and reporting of the actual costs and time and any variance to date.

The eCIMS Project Plan provides for four levels of monitoring and control over the development. The first three are daily, weekly, and monthly tracking of problems and their resolution, and progress against the Plan. The fourth is a quarterly review and, if needed, revision of the Plan itself. The monitoring and control are being overseen by the Project Authority and the eCIMS Steering Committee. As already noted, it is our opinion that, while it has an important role to play in guiding the progress of the project, the eCIMS Steering Committee is neither structured nor positioned to provide corporate governance.

Recommendation:

2. The eCIMS Project Manager should estimate the cumulative costs and elapsed time for all major milestones, including the pilot and the additional development that will be required subsequently to implement the system across both Councils. The costs should address both the development and the maintenance of the system (life-cycle costs).
3. The eCIMS Project Authority should report formally to the joint NSERC and SSHRC eCIMS Governance Committee on the progress of the development against the plan and alert the Committee to variations in the expected deliverables and cost and time schedules. The reporting should occur periodically and at major milestones in the project.
4. The joint NSERC and SSHRC eCIMS Governance Committee should consider the cumulative actual costs and elapsed time, and the life-cycle costs in making decisions on the project.

3. Increased user representation in all phases of the project, including the limited implementation pilot.

Observation

The eCIMS Project Plan and Limited Implementation Pilot Plan provide for an Information Management Working Group to provide advice and guidance on the configuration and use of the system. This group comprises all the managers from the IM section and a member from ISD. In addition, there is a User Group representing the rest of the Councils to provide feedback on performance and possible improvements. This group, however, is scheduled to participate only in February 2005, when it will help evaluate the pilot project.

In addition, the project is implementing a Communications Plan that will disseminate information on the project and the system to the various audiences in the Councils: management, user groups (e.g., eBusiness, NAMIS, AMIS), Council staff, and IM. Through its communiqués, the project expects to build IM awareness and buy-in among the potential users of eCIMS. While this action will be very useful, it will not address the users' need to be consulted: Communication is a two-way street.

Users need to be more involved on an ongoing basis in determining the scope of the system and their priorities from an organizational and management standpoint, and in defining, testing, and approving the system's functional and control requirements. Involvement from the onset of the pilot will also prepare the users for their ongoing role through the system's full implementation and life-cycle.

We understand that, to address these risks, the project is considering a phased approach that will ensure appropriate user representation through the course of the development.

Discussion

User Involvement in COTS

In acquiring iRIMS in 2002 and subsequently the Livelink records and document management systems in 2003, the Councils adopted a commercial off-the-shelf (COTS) application system. The use of a COTS system is considered a good practice for managing the risks of a system development project. The many advantages to using COTS components include lower purchase cost, immediacy of acquisition, greater ease of modernization, and reduced development costs. The project has reduced the programming risks by deciding to install the Livelink systems as is, without any modifications. This decision also facilitates better support from the system's supplier, Open Text.

COTS systems, however, also carry risks, which must be managed as rigorously as those of an in-house development. One of these risks is that the system's implementation will be effected without appropriate user participation. If users are not involved in the project along with management, the system that is developed may not meet their needs; and feeling rejected, the users may abandon the project and the system that it delivers. If users are not involved in the design of adequate input, processing, and output controls, the system may not ensure the confidentiality, integrity, and availability of the information it processes.

Furthermore, as noted by Carnegie Mellon University's Software Engineering Institute (SEI) in "COTS-Based Systems Lessons Learned," the use of COTS products will likely require changes in the users' business processes. Sometimes, the organization's current practices are more advanced than those reflected in the COTS product. In this case, it may be possible for the organization to work with vendors to bring their products up to the advanced processes. It is important, therefore, to involve users in determining which business processes can and should be changed. This challenge is enhanced by the existence of the two sets of users that constitute the Councils.

User Involvement in the Limited Implementation Pilot

As already noted, the eCIMS project is planning a limited implementation pilot to test, validate, and confirm the system's configuration for use in the Councils. We appreciate that the project has intentionally restricted the pilot to the Administration Division of CASD in order to focus the implementation and keep it manageable and efficient. On the other hand, the pilot's limited scope within a single site poses the risk that the user community's perspective, especially in the program areas, may not be completely and accurately represented. Furthermore, the criteria developed to assess the results of the pilot may not reflect the user community as a whole.

Recommendation:

5. The eCIMS Project Manager should involve a cross-section of the potential user community, including the program areas, from the start of the pilot so that users get to feel and be a part of the process.
6. The eCIMS Project Manager should establish and communicate the users' roles and responsibilities in defining, testing, and accepting the system's functional and control requirements.

4. Use of an appropriate system development methodology (SDM) for all phases of the project, including the limited implementation pilot.

Observation

The eCIMS project is using two proven techniques to reduce the risk of the development: a commercial off-the-shelf (COTS) system and a limited implementation pilot. In addition, the project has obtained a dedicated ISD member as part of the project team and defined the following appropriate roles and responsibilities for ISD: help create the Project Plan; train project office staff; transfer knowledge from ISD to CIM; develop the pilot project plan and preliminary Threat and Risk Assessment (TRA); conduct quality assurance; rollout and evaluate the pilot project; transfer knowledge from the Project Office to eCIMS support; complete the TRA and Privacy Impact Assessment; and then deploy the system across the Councils. ISD will maintain the production and development environments, provide technical support for the system (i.e., Helpdesk), support CIM in receiving and tracking non-technical issues, and provide advice and direction on the IT security policy and practices. The eCIMS Limited Implementation Pilot Project Plan, November 5, 2004, reinforces the role of ISD in the development.

To ensure their effectiveness, however, ISD's efforts need to be managed through an appropriate system development methodology (SDM).

Discussion

The SDM is the process, involving multiple stages (from establishing the system's feasibility to carrying out post implementation reviews), that is used to convert a management need into an application system, which may be custom-developed or purchased or a combination of both. A sound SDM guides the efforts of the development team and helps to ensure that all phases of the project are consistently performed according to accepted standards, while offering flexibility of use on projects of varying scope and complexity.

Without a sound methodology, there may be more operational, program, and user initiated errors. Poor design or conversion procedures and incorrect user operation may result in the processing of incomplete or inaccurate information. If appropriate standards are not followed in installing, configuring, and maintaining the system, it may prove unreliable and costly to operate. A system that is poorly designed may result in erroneous or inefficient processing of information and pose significant risks to the organization's assets and operations.

SDM and COTS

As noted, the use of a COTS system by the project is considered a good practice for managing the risks of a system development project. The many advantages to using COTS components include lower purchase cost, immediacy of acquisition, greater ease of modernization, and reduced development costs. The project has reduced the programming risks by deciding to install the Livelink systems as is, without any modifications. This decision also facilitates direct support from the system's supplier, Open Text.

COTS systems, however, also carry risks which must be managed as rigorously as those of an in-house development. For example, the in-house programming staff may be less familiar with the application, resulting in an increased learning curve for ongoing support and maintenance. The vendor may not be stable, increasing the chances of inadequate support of the product. The vendor's documentation may be inadequate for ISD to operate and the Councils to use the system properly.

As observed by Carnegie Mellon University's Software Engineering Institute (SEI), there is a need for an engineering process when developing a system based on COTS products. One cannot make any assumptions about traditional activities such as requirements analysis or preliminary design. Reducing or omitting an activity should only be considered after careful analysis of the impact on the program. Even configuration or customization of COTS systems takes time and effort. The customization of COTS products is a part of system configuration, integration, and installation and, as such, can become invisible if not adequately documented. Furthermore, COTS configuration and integration activities can require as much attention to code and language as traditional development activities. It also continues to be important to define and validate interfaces to external systems. Whereas in a custom-developed system one may be able to make up for inadequacies in the interfaces, one's control of how COTS products interface with other systems (or even parts of the system) is non-existent.

SDM and the Limited Implementation Pilot

As noted, the project is using a limited implementation pilot to help management determine whether the technology meets the Councils' needs. Such a phased approach is considered a good practice for limiting the risks of system development. To be effective, however, the pilot too must be managed properly.

The eCIMS Limited Implementation Pilot Project Plan notes that the pilot will provide the opportunity for stress testing the system with live data and for creating and revising training, maintenance, and support procedures before the system is implemented across the Councils. It states that CIM will be responsible for daily testing the integrity and validity of existing and new information products used by the Councils and compiling and maintaining statistics regarding system performance and capacity. The integrity and validity testing will assess whether the information can be retrieved and displayed by the system.

The Plan does not specify the other criteria needed to determine whether the pilot is a success. These criteria should encompass the project itself, the system's functionality, the data it processes, and the information it reports. For example, it should consider the cost-benefit of the system (the assumptions versus actual); policy and guidance on the information to be managed through the system; delivered functionality (for example, search capabilities, retention and disposition rules, record review, access control, document sharing, and workflow approvals); functionality versus users' requirements; integration with the Councils' systems; and documentation. The development of appropriate criteria, the tests to be used to exercise them, the expected results, and the methodology to collect the related data must be completed properly before the start of the pilot.

Recommendation:

7. To ensure that ISD guides the efforts of the development team and helps to make sure that all phases of the project are performed consistently according to accepted standards, the eCIMS Project Manager should formally engage ISD's expertise in employing an appropriate system development methodology to guide the development, implementation, and maintenance of eCIMS, including the limited implementation pilot.

Appendix A

Auditor’s Risk Assessment of the eCIMS Development Project

As stated in the Business Case, April 5, 2004, the eCIMS development project is tasked with developing and implementing an electronic information management (IM) solution for use by NSERC and SSHRC.

The objective of a development project is to deliver a system that meets the clients’ needs and expectations, with minimal defects, in the shortest calendar time, and at the lowest life-cycle cost. Risk is the possibility of an event occurring that will have an impact on the achievement of objectives. There are, therefore, two kinds of risks associated with the system development process: Project Risks and Technology Risks.

Project risks are related to the management of the project, including the management of change, and encompass:

- Improper scope. An improperly or inadequately defined project scope may result in a system that provides insufficient or unneeded functionality to the organization; disrupts the project plan and schedule; and wastes both human and financial resources.
- Cost and time overruns. Without proper planning and monitoring, the project may be implemented late and at a greater cost than expected.
- Unsatisfied user needs. If users are not involved in the project, the system that is developed may not meet their needs; and feeling rejected, the users may abandon the project and the system that it delivers. The risk is enhanced by the existence of the two sets of users that constitute the Councils.

Technology Risks are related to the system that is being developed and include the following:

- Inadequate functionality, usability, and performance. Without adequate user involvement in the development, the system may not deliver the expected functionality. Without a sound methodology and user support, there may be more operational, program, and user initiated errors. Poor design or conversion procedures and incorrect user operation may result in the processing of incomplete or inaccurate information.
- Problems in maintainability. If appropriate standards are not followed in developing, installing, and maintaining the system, it may prove unreliable and costly to operate.
- Poor system controllability. If users are not involved with the project team in the design of adequate input, processing, and output controls, the system may not be able to ensure the confidentiality, integrity, and availability of the information it produces.
- Inappropriate technology. Without the participation of a qualified member from the IT organization, the system that is developed may not fit the organization’s IT infrastructure, be unsupportable in-house and, consequently, be wholly dependent on vendors or consultants for its operations and maintenance.

- Problems in implementation. A system that is poorly designed may result in erroneous or inefficient processing of information and pose significant risks to the organization’s assets and operations.

These risks informed the definition of the audit’s Objective, Scope, Criteria, and Methodology.

Appendix B

Audit Criteria

The audit criteria to assess how well management is addressing the project and technical risks for eCIMS:

- Have been derived from "Managing Information and Developing Systems, Systems Auditability and Control Report," the Institute of Internal Auditors (IIA) and "COTS-Based Systems Lessons Learned," the Software Engineering Institute (SEI).
- Are consistent with the approaches contained in the "Report on Systems under Development" and "System under Development: Getting Results," Office of the Auditor General of Canada (OAG).

The audit criteria comprise the following:

Adequate Management Commitment, Change Management, and Control, in each of the two Councils

1. Management participates throughout the lifecycle of the project.
2. Management commits human and financial resources needed for the project.
3. Management approves the project plan with its documented detailed objectives, scope, methodology, risk management strategy, deliverables and their milestones, and related approval points.
4. Management establishes and implements a change management strategy for eCIMS:
    a. Communicates a sense of urgency for the project and the system.
    b. Creates a cross-functional leadership team to guide and sponsor the eCIMS throughout the Councils.
    c. Develops a clear vision for the eCIMS.
    d. Communicates the vision frequently throughout the Councils.
    e. Empowers employees to work towards the vision by removing barriers to action.
    f. Achieves and recognizes short term successes to show that change is working.
    g. Consolidates successes and keeps the project moving.
    h. Anchors or embeds the change within the organizational culture.
5. Management monitors the progress of the development against the plan, reallocates resources as necessary, reprioritizes the plan to coincide with changing conditions and organizational objectives, and determines the performance and functional requirements for baseline controls.

Adequate User Participation in Requirements Definition, in each of the two Councils

6. Users help to determine the scope of the system and their priorities from an organizational or management standpoint, define the system's functional and control requirements during the analysis phase, and test and approve the functions and controls before implementation.
7. Users are involved in choosing the technology and approving its functionality and controllability.

Adequate Project Management

8. The project manages the risks that threaten the achievement of its objectives:
    a. Improper scope.
    b. Cost and time overruns.
    c. Unsatisfied user needs.
9. The project conducts proper reporting that allows management to monitor progress and alerts management to variations in the expected deliverables and time and cost schedules. The reporting occurs periodically and at key points or milestones in the project.

Adequate Information Systems Division (ISD) Participation

10. The ISD assists in the selection of the appropriate technology, assesses the technological risks, participates in the assessment of the business risks, and designs appropriate controls with the users.
11. ISD assists the users in implementing the system from a technical standpoint.
12. ISD is involved in planning for the system's performance and in identifying requirements for performance objectives.

Adequate Quality Assurance

13. The project uses a Quality Assurance (QA) function for all its phases.
14. QA assists in the assessment of the quality of the controls surrounding the development of the system and the controls within the system. QA ensures that the system satisfies the control and security requirements of the organization.

Appropriate System Development Methodology

15. The project uses a sound system development methodology (SDM) to guide the efforts of the project team and to manage the project's phases. The SDM addresses the following:
    a. At the initiation phase, the cost-benefit analysis and project approval.
    b. At the analysis phase, requirements, process, data, and technology definitions.
    c. At the design phase, process, data and technology design, and data conversion.
    d. At the construction phase, programming procedures and documentation, user procedures and documentation, and testing.
    e. At the implementation phase, training, implementation, and user acceptance.

Appendix C

Audit Methodology and Approach

The audit methodology included interviews with relevant persons in CASD, Administration, CIM, eCIMS project team, ISD, NSERC Operations Committee and NSERC and SSHRC Management Committees, and prospective users in corporate services and the program areas of the two Councils; review of appropriate documentation such as the business case, project work plans, project documentation, project status reports, IM Strategic Plan, Committee meeting minutes, and cost and budget schedules; and a review of the eCIMS functionality.