Health Canada | Santé Canada

Final Audit Report

SAP General Controls

September 2011

Table of Contents

Executive Summary

Financial management systems are essential to the management of government operations. These systems are designed to enable strong financial management of public resources, to reinforce the principles of probity and prudence and to contribute to better decision-making (within each department and government wide). Today, SAP Enterprise Resource Planning is the "choice" software used widely across the Government of Canada as well as across the private sector.

The objective of the audit was to assess the effectiveness of Health Canada's general controls for SAP. While Health Canada is the SAP host for a cluster of five other organizations, the audit focussed solely on the system and data at Health Canada. The audit was conducted by the Audit and Accountability Bureau and sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing.*

SAP, as an enterprise financial and material management business solution for the Government of Canada, has significant support both within Health Canada and across the government community. The control environment for SAP management and operation within the Department is clearly evident and shows evidence of following the set government direction. Within that control environment, a separate organizational unit exists with the specific mandate of managing the SAP operation – roles and responsibilities are defined and employees are aware of their accountability. A collaborative partnership between business and information technology teams has developed to address SAP operations in an integrated manner.

SAP changes are managed as a process by both the business team and the IT team. While the teams have previously implemented significant SAP changes, going forward they would benefit from improving the change management process to accommodate the larger SAP changes.

Control over user accounts is functioning well, however the SAP team would benefit from strengthening the area of granting Special Access privileges and aligning user account expiration dates for temporary users with term or contract end dates.

The overall batch control framework is designed to preserve the integrity and authenticity of external application data processed by SAP. However, there is a segregation of duties concern between SAP online and batch transaction processing. The specific issue concerns end-users who have both access to SAP and the capability to enter transactions that are processed by SAP through a Branch feeder system. In addition, batch balancing controls are not employed for Health Canada feeder files, meaning that the accuracy and completeness of transaction data cannot be verified.

Security in the SAP operation is managed following the direction set by the government, nonetheless, the existing Threat-Risk Assessment (TRA) is out of date and should be re-visited. In addition, tests of segregation of duties conflicts should be strengthened as a few potential segregation of duties conflicts had not yet been detected by the SAP team. Although the audit detected this concern, the full scope of this issue will require further work from the SAP team.

Management agrees with the four recommendations and has provided an action plan that will serve to strengthen the general controls for SAP at Health Canada.

1. Introduction

1.1 Background

The Integrated Financial and Materiel System

Financial management systems are essential to the management of government operations. These systems are designed to enable strong financial management of public resources, to reinforce the principles of probity and prudence and to contribute to better decision-making (within each department and government wide). Overall, a well designed and managed system should provide efficiency and effectiveness resulting in savings. Today, SAP Enterprise Resource Planning is the "choice" software used widely across the Government of Canada as well as across the private sector.

The Government of Canada has a centre of expertise for commercial products that combines finance, materiel management, assets, salary management, project management and other functionalities; this specifically includes the SAP software product. It is a service organization that provides a wide variety of support and development services to the federal government thereby allowing departmental staff to focus on core business functions while reducing departmental investment in application development, systems maintenance and training. Essentially, the Centre assists departments in meeting Government of Canada priorities by leveraging a common software product, developing standard tools, and providing departments with standardized reports to meet departmental and Government of Canada reporting requirements.

The Centre is commonly known as the Integrated Financial and Materiel System Cluster and is the largest shared system cluster operating within the Government of Canada. It is a body of organizations that work together to leverage efficiencies and participate in common system development and procurement activities based on shared business rules. Department members work toward a common goal with shared resources to optimize overall enterprise gain. Health Canada has been a member of the cluster group since its inception.

At Health Canada there are key feeder systems such as; grants and contributions, revenue invoicing, human resources and travel services which transmit batches of transactions for processing in the financial system (SAP). In turn, the SAP system feeds data into internal systems for financial reporting and analysis. Departmental financial information in SAP flows to and from the Government of Canada's financial systems.

IT Control Framework

In business and accounting, **Information Technology controls** (or **IT controls**) are specific activities performed by persons or systems; the controls are designed so that business objectives are met. Essentially, IT controls are a subset of an organization's internal controls. IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function. IT controls are often described in two categories: IT general controls and IT application controls. General

computer controls include controls over the IT environment, computer operations, access to programs and data, program development and program changes. IT application computer controls refer to transaction processing controls sometimes called "input-processing-output" controls. The focus for the audit is on the IT general computer controls.

1.2 Audit Objective

The objective of the audit is to assess the effectiveness of Health Canada's general computer controls for SAP with a focus on governance, managing system change and security.

1.3 Scope and Approach

The focus for the SAP general controls audit included: governance and oversight; system change management and operational controls; and security safeguards. While Health Canada is the SAP host for a cluster of five other organizations, the audit focussed solely on the system and data at Health Canada.

The engagement was carried out at headquarters and involved interviews with staff within the Chief Financial Officer Branch (including the Internal Controls Division and the Framework for Integrated Resource Management Systems (FIRMS)). Interviews were also conducted with the FIRMS IT Development and Support Team within the Corporate Services Branch. The engagement also included an examination of selected documentation, operating procedures and related SAP technical configurations. The audit examination was limited to financial data recorded in SAP by Health Canada branches and programs for the fiscal year 2009-10.

The Control Objectives for Information and Related Technology Framework (COBIT) is a widely-used framework promulgated by the IT Governance Institute, which defines a baseline of IT general computer controls and application control objectives with recommended evaluation approaches. COBIT was used as a source of best practices in this audit.

1.4 Statement of Assurance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*.

2. Findings, Recommendations and Management Responses

2.1 Governance and Oversight

2.1.1 Oversight

Audit Criterion: *An appropriate governance body (steering committee) has been established to prioritize IT investments for the SAP operation and supporting infrastructure.*

Health Canada is a member of the Integrated Financial and Material System (IFMS) Program, a Shared Services system cluster supporting SAP technologies within the Government of Canada. It operates within a multi-tiered governance structure with member departments being represented at all levels.

- **IFMS Steering Committee** - the senior-level body that has accountability for the success of the IFMS Program and its strategic alignment with federal government objectives. It is comprised of senior executives from each of the member departments and is similar to a Board of Directors.
- **IFMS Management Board** – recommends strategic and funding decisions directly to the IFMS Steering Committee. It is similar to an Executive Committee.
- **IFMS Operations Board** – the technical/operational oversight group reporting directly to the IFMS Management Board. It makes functional decisions and recommendations to the IMB.
- **IFMS Forums** – are aligned according to SAP functions and are the source of operational subject matter expertise. The forums report to the IOB and are responsible for providing operational support and input on functional issues.
- **IFMS Program Office** – is the service organization that reports directly to the management board and provides advice, assistance, and support to all governance levels. Services provided include: procurement of products, product research and testing, applications, enhancements, technical support, coordination and secretariat support for committee and forum meetings including agendas and minutes, communications, documentation, and training. This group has developed a control framework that has been endorsed and implemented by Health Canada.

The IFMS governance structure guides, directs, and supports the ongoing IFMS Program delivery across government. The strategic direction, priorities, multi-year plan activities, and budgets are established for the IFMS program and approved by its Steering Committee. The approved strategic focus for 2011-14 is on standardization, business evolution, IFMS community, and cluster expansion. Standardization projects include: establishing a schedule with departments to move to the same up-to-date version of the package; stabilizing what that up-to-date package entails; and, reducing the number of cases where departments have deviated from the norm. The business evolution includes

building and implementing new business functionality, but at a slower pace. IFMS community includes optimizing training for SAP experts and users for all departments.

Health Canada representatives actively participate on the committee, boards and forums of the IFMS program. For each committee, agendas are prepared by the IFMS Program Office and are distributed to members. The minutes distributed include approval of agenda and previous minutes, a review of action items, and decisions taken. Overall, Health Canada, by participating in the cluster processes, continues to support the priorities and direction of the Government of Canada's IFMS program.

Health Canada Oversight

As the business owner of SAP, the Chief Financial Officer Branch (CFOB) is the departmental point of accountability to ensure that the SAP system provides rigorous stewardship of resources and good information in order to manage for results. The Branch provides the necessary enabling frameworks, policies, systems, practices, and tools to support program management and operations. It ensures compliance with government financial policies and regulations. Decisions for the operation and support of the SAP product at Health Canada follow the departmental governance structure. As a result, all major IT projects, including major changes/releases to the financial system, must now be part of the Investment Plan. The Chief Financial Officer Branch has a series of committees that provide governance for the financial system and its processes.

The Accounting Operations and Systems Division is accountable for the transactional and financial systems support to the Department. The Division's role encompasses a number of distinct services provided by the various organizational units. A specific unit, the Framework for Integrated Resources Management Systems **(**FIRMS) within the Accounting Operations and Systems Division, has the mandate to ensure the Department's financial and material management system (SAP) is fully operational.

In partnership, the Corporate Services Branch - Information Management Services Directorate (IMSD) provides the departmental strategy, policies, infrastructure, tools and personnel to make effective use of information management and information technology in the delivery of departmental programs and services. This includes developing, implementing and communicating policies, standards and guidelines; and facilitating the planning and delivery of corporate projects including on-going support and maintenance. Within the Solution Centre – Corporate Applications and Systems provides these services to support the Department's financial and material management system (SAP). The FIRMS Application Development and Support team is co-located with the FIRMS business group and is dedicated to keeping SAP operational.

The FIRMS functional unit, as part of its annual operational planning process, identifies any required upgrades or projects. For fiscal year 2010-11 the SAP functional Team submitted two projects to be supported: the SAP upgrade and the SAP Project Systems / Cross Application Time Sheet modules (SAP PS / CATS). Both projects were included within the approved list of IT projects for 2010-11. The SAP upgrade was divided into

two phases. The first has been implemented and the second is slated for implementation in 2011-12.

Health Canada has a governance structure under which decisions are made; this structure is followed for SAP-related decisions. In addition, the Department follows the leadership of the Government of Canada's IFMS Cluster.

2.1.2 Roles and Responsibilities

Audit Criterion: *Roles and responsibilities related to SAP systems have been clearly defined, documented and understood.*

Responsibilities for the Departmental Financial Management System (SAP) are split between the functional (under the Chief Financial Officer) and the technical (under the Chief Information Officer (CIO)). The functional team is responsible for the business processes and the help desk support related to the business processes, the training of the end users, documentation and testing of new business processes or changes to existing processes. The technical team is responsible for the hardware, infrastructure, software development and support of the application.

The SAP product is designed in several modules, each with specific business functions. FIRMS is organized into eight business teams that provide functional support for the SAP modules that have been implemented and are being used by Health Canada. In addition, teams exist for client services and liaison, and system integration. Client services include administration of user accounts and security profiles within the application. Roles and responsibilities are documented and further supported by business processes and workflow documents. However, it is not clear from documentation reviewed if these roles and responsibilities have been formally approved by management.

The Corporate Applications and Systems SAP team, called the Application Development and Support – FIRMS or simply FIRMS-IT, is specifically responsible for collaborating with the FIRMS teams to ensure business functions and deliverables are operational. Their functions include: implementing and maintaining the automated equipment, operating systems, data bases, and applications (e.g., SAP), and providing application development services to meet FIRMS business objectives. The FIRMS-IT team is divided into three distinct groups; programmers, technical support, and security. The co-location and integrated day-to-day operations of the FIRMS business team with the IT team has resulted in an excellent working relationship.

Through the combined effort of the two teams, they manage over 4,000 SAP user accounts of which approximately 2,300 are Health Canada users. The remaining accounts are Health portfolio or external users hosted by the departmental SAP operation. The roles and responsibilities for the administrators and users have been documented in training material as well as other manuals. Significant effort is made to support these users and to ensure segregation of duties so risk can be minimized.

With respect to the ongoing operations and support of SAP, roles and responsibilities are defined and employees are aware of their accountability. The integrated nature of work between FIRMS business and IT teams has resulted in a necessary collaborative partnership.

2.1.3 Monitoring and Management Reporting

Audit Criterion: *Management has established regular monitoring specific to the SAP operation.*

The FIRMS group holds weekly meetings between the business staff and the FIRMS IT support team to ensure issues are raised and discussed. FIRMS staff maintains minutes of these meetings, any records of decision and resulting actions. Regular meetings take place between the Manager, FIRMS and the Director, Accounting Operations and Systems Division to communicate any significant issues.

On an annual basis, as part of the departmental planning process, FIRMS staff develops an operational plan. While the team reports against the plan every month, the Department has not otherwise established performance standards or benchmarks for SAP. The operational plan for 2011-2012 includes some key significant activities including the upgrade of SAP to version 6.0 as well as enhanced SAP features to support the Cost Recovery Initiative – both are included in Health Canada's Investment Plan. In addition, an internal review of the organizational structure of the FIRMS Team is planned to ensure it is structured in the best way to support the different stakeholders.

The FIRMS group has begun to prepare for the SAP upgrade by providing for the support of a Project Manager. The Project Manager will be tasked to: prepare a project plan; provide advice on change management; and develop communication and training strategies. The FIRMS functional team and IT team will work towards the completion of this project by the end of the calendar year.

In addition, during the audit it was noted that the Director, Accounting Operations and Systems Division, the Director, Corporate Applications and Systems, the Chief of FIRMS and the Chief of FIRMS-IT meet every three weeks to review and monitor progress on key financial system initiatives and discuss issues / risks that have been identified.

2.2 System Change Management and Operational Controls

2.2.1 SAP Change Management

Audit Criterion: *Documentation exists to support approval by a delegated authority for all software development and changes.*

SAP change procedures and standards are critical for ensuring the accuracy and integrity of the Department's financial information. The value of this information is dependent on the ability to respond and prioritize requests for change caused by government-wide and departmental policy decisions. Value is measured by the continuity and reliability of the information stored in the Department's financial system.

Business processes and workflows designed by FIRMS for managing changes to the SAP software are well documented. Between the FIRMS functional team and the IT support team, there are a number of documents and process diagrams that clearly communicate responsibilities and the overarching process and sub-processes that make up the Department's SAP Change Management process. Both Teams have also adopted sound configuration management practices via toolsets which have the capacity and capability to record, track and report.

Tool Set Capacity and Capability

WHO is the **R**equestor?
WHO is **R**esponsible for the development, quality assurance and final change implementation?
WHAT is the **R**eason for the change?
WHAT is the expected **R**eturn from the change?
WHAT **R**isk factors are associated with the change?
WHAT **R**esources are required to execute the change?
WHAT is the inter-**R**elationship between this change and other changes?

Audit tests indicate that when system changes are small in scope the workflow processes and change documentation include appropriate evidence of impact analysis and change testing being conducted in support of the enhancements and fixes. However, the level of documentation for some large-scope changes to substantiate appropriate testing, impact analysis, planning and prioritization could be strengthened.

While the Department has a change management process, it is important to have all aspects of the process working effectively to allow for quality assurance before migrating changes into production. Without appropriate evidence of the process being completely followed, there is a risk that significant SAP changes may not be implemented on time. For example, in 2010-11 Health Canada implemented the Unicode conversion in preparation for the SAP upgrade to version 6.0. The Unicode conversion affected all SAP program components. However, there was no formal project regime to demonstrate fixed timelines and there was limited evidence of resource allocations. The Department is currently preparing for the next steps of the upgrade to version 6.0 and, while the FIRMS - functional team is engaging a project manager with SAP upgrade experience, it will be important that the Department adopt a project management discipline.

While the FIRMS group has previously implemented significant SAP changes, going forward they would benefit from improving the change management process to accommodate large SAP changes as well as the day to day maintenance. This should provide a more complete trace of change management actions taken as well as capture existing corporate knowledge in the event of the loss of experienced resources.

2.2.2 SAP User Account Management

***Audit Criteria**: User account and role privileges are authorized by a delegated authority and audit trail records are retained.*

Critical and confidential information should only be available to those with access. This can be accomplished by managing user accounts to maintain the integrity of information

and processing infrastructure. The SAP product controls access to its business transactions and resources using a complex hierarchy of authorization objects; authorization methods; profiles and composite profiles (for multiple function users).

Health Canada provides access to the financial system through the management of user accounts which can be generalized into four user categories: end users; temporary users; FIRMS users; and technical support users.

The FIRMS functional team owns the business processes supporting SAP access control, while the Client Services and Training group is responsible for delivering the services of account maintenance for all four SAP user categories. Business processes and workflows designed to administer and control access to SAP are similar to those adopted for change management. These processes are well documented and clearly communicate responsibilities, workflow definitions and documentation requirements for each user account (audit trail). These processes are functioning well.

The audit examined key controls in the SAP User Account Maintenance workflow where appropriate authorization is required to obtain access privileges to SAP. Special access Requests are used largely when some form of trouble shooting action is necessary. This form of access is most often requested by members of the SAP technical support, programming, or security teams. As special access requests can be high risk, these events must be logged, monitored, and closed out in a timely fashion. Weekly reports are produced on all such requests. Since 2010, there have been 175 requests for special access; these access requests were recorded, monitored and closed appropriately. This procedure represents good compensative and preventive control over the most common system security threats/vulnerabilities relating to the user account and user authorization assignment activities carried out by FIRMS. Nonetheless, text describing the purpose and/ or objective of "Special Access Requests" is sometimes vague and not consistently filled out to provide the reader with contextual understanding of the reason or requirement. Audit test results illustrate that there is generally not enough information recorded in the request to make an informed decision nor is there documented evidence to prove or disprove a security review has taken place.

Technical support users require profiles that enable them to perform technical development and support activities. Occasionally, members of the technical support team are required to make changes to database tables containing master or control information on a scale that exceeds the threshold of proper segregation of duties access limits. The User Trace feature, which provides the capability to verify that temporary “special access” privileges were used for its intended and authorized purpose, was either not turned on or was not included in the documentation in 50 percent of the tests.

In addition, expiration dates set for user accounts do not conform to a consistent standard. More specifically, expiration dates for temporary and contract staffs are arbitrarily set 20 years into the future from the start date.

While overall the control over user accounts is functioning well, FIRMS would benefit from strengthening the area of granting special access privileges and aligning user account expiration dates for temporary users with term or contract end dates.

Recommendation 1

It is recommended that the Assistant Deputy Minister, Chief Financial Officer Branch strengthen control over user accounts related to SAP operation, including the tracing of special access privileges and setting user account expiration for term/contract staff.

Management Response

Management agrees with this recommendation.

While the form for special access requests does not always provide the full details on the purpose of the requests, other documentation and communication outside of the form provide the context and rationale for the requests in the form of emails or verbal communications. The additional information provides the approver with enough information to make an informed decision. Going forward staff will be reminded to include, text describing the purpose and/or objective of special access requests within the form. SAP Security will update their procedures to include the turning on of the "User Trace" feature and to copy the results in the Special Access Request form.

FIRMS will create a development request to have the SAP User Access Request Form modified to include "Employee Status" such as Indeterminate, Casual, Term or Contractor and include the employment or contract end date to input as the expiration date in the user account for temporary staff and contractors.

In the short term, FIRMS will request the Branch SAP security officers to use the comment field to provide the status of the user (i.e. employment status or contractor) and the related expiration dates when required.

2.2.3 Batch Controls

Audit Criterion: *Batch control procedures and exception processing are implemented to provide assurance that data processed by SAP is valid, accurate and complete.*

Batch controls are a method used to manage high volumes of transaction data through a system. They provide assurance that all records in the batch are processed and that no records are processed more than once. Batch controls also provide an audit trail of transactions. Health Canada's existing financial systems generate transaction data such as vendor invoices and Grants and Contributions commitments to be processed by SAP. This data is transmitted in batches that are called "feeder files". Batch controls help ensure that automated business transactions are valid, accurate and complete.

Health Canada's SAP batch file processing schedule consists of over 60 inbound and outbound files. The majority of these interface files are inbound files - ranging from Pay File Control Data and Account Balance reports to Interdepartmental Settlement files. Also included in the schedule are seven inbound Health Canada branch feeder files.

Audit testing of batch controls was restricted to incoming branch feeder files. The overall control framework for batch processing allows files to be transmitted over secure connections and come from recognized sources. In addition, there are safeguards against unauthorized changes and standard notification of submission and exception reporting. For example, feeder files are encrypted while in transit. The security protocol used is widely evident and well designed with respect to preventing eavesdropping on files in transit and avoiding attacks where files are intercepted.

Every 15 minutes the SAP server pulls these files in for automatic processing by the SAP batch system. As a compensatory control, access to file transfer locations is restricted to authorized Branch Program staff. In addition, automatic notification of batch processing results and exception reporting are sent through the Health Canada email system to FIRMS. These automated processes notify the FIRMS teams of the processing results, such as the listing of files processed, disposition of files (success/failure) and description of any failures. Roles and responsibilities of the IT support and functional business teams specify monitoring of all batch jobs and file transmissions for the SAP environment.

While these controls are in place, there is an access issue that increases the risk that inaccurate or incomplete data may be processed in SAP. The specific issue is around the segregation of duties [Exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b)] The Security Monitoring in the SAP section of this report covers the segregation of duties more fully.

Industry "best practices" recommend the implementation of detective controls to validate the accuracy and completeness of electronic file exchanges using batch balancing controls. These controls require that header records are transmitted along with transactional data in order to provide the receiving organization with a means to reconcile transaction data

received. Such controls might include record counts, control totals of dollar amounts, and hash totals of non-dollar numeric data. [Exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b)] The audit team examined the inbound external pay files and found that they do include batch balancing controls such as *Record Counts* and *Hash Totals*. Audits conducted in 2006 and 2007 on five feeder systems concluded that in two cases completeness of data shared between these systems and SAP could not be determined due to the lack of control totals. As a result, reconciliations were implemented in these cases as an interim measure until new systems could be implemented. Reconciliations will detect control issues after SAP processing; batch controls will detect control issues before batches are processed in SAP.

The overall batch control framework ensures the integrity and authenticity of external application data processed by SAP. The Health Canada – SAP environment ensures users are known, secures access to file transfer locations and uses secure transmissions. However, there is a potential segregation of duties concern between SAP online and batch transaction processing. The control over incoming batches can be strengthened to protect the accuracy of SAP data.

Recommendation 2

It is recommended that the Assistant Deputy Minister, Chief Financial Officer Branch improve control over batch file processing in SAP by changing SAP batch interface requirements to include implementing batch balancing totals.

Management Response

Management agrees with this recommendation.

As noted in the report, reconciliations have been implemented to ensure the completeness of data between internal Health Canada (HC) feeder systems and SAP. These reconciliations provide assurance on the completeness of data and mitigate the risk. Given the plans to replace the Department's two Grants and Contribution applications with one system, it would not be cost effective to implement new batch interface requirements at this time. FIRMS will update their generic batch file interface requirement documents to include batch balancing totals. The new requirements will be implemented for any new interfaces developed or when changes are made to existing interfaces with internal HC feeder systems.

2.2.4 SAP Operational Controls

Audit Criterion: *Procedures related to SAP operations have been defined to effectively manage and monitor scheduled processes to ensure the accuracy of data processing activities.*

FIRMS has the mandate to ensure that upgrades (new releases), enhancements and maintenance are implemented for SAP. The FIRMS-IT team's roles and responsibilities are formalized, well documented and up-to-date. The team has developed technical

documentation that clearly illustrates how batch file transfers take place, the physical equipment inventory and logical connection of SAP and related equipment, development and production transport (implementation) paths, and end client access points.

The FIRMS-IT team has also recently made improvements to the detective controls within the monitoring schedule and activities by implementing automated notification via email for application and system alerts. Alerts occur when situations are detected regarding the operation of SAP that are deemed to be out of the norm. There are four dedicated staff resources continually monitoring logs of activity regarding SAP infrastructure and servers ready to respond to automated notification of system and application alerts. Examples of the infrastructure logs and reports monitored by the team include:

- storage availability and overall computer usage;
- infrastructure operations such as inspection of Oracle database components;
- database maintenance such as index administration and backup;
- SAP application server status and operational health;
- nightly batch job processing and exception reporting.

Procedures directly related to SAP operations have been defined and designed to effectively manage and monitor scheduled processes to ensure the accuracy of data processing activities. In this way, the FIRMS-IT support team can ensure that IT services are available as required.

2.3 Security Safeguards

2.3.1 SAP Security Set-up

Audit Criterion: *The SAP configuration settings, certification and accreditation process, and assessment of environmental vulnerabilities comply with TB and departmental operational security standards and objectives.*

In most computer environments, formal methods must be applied to ensure that the appropriate computer information system security safeguards are in place and that they are functioning according to specifications. Safeguards are important to protect the environment and the specific system from unauthorized access, alteration or destruction. According to the Treasury Board of Canada Secretariat and to the departmental security policies and operational security standards, risks to the Department's computer environment involving a specific system are to be analyzed as early as possible in the development process so that planned responses can be evaluated for all Health Canada systems and applications being developed or updated. These analyses are called Threat and Risk Assessments (TRAs).

Overall, a secure environment has been created within Heath Canada for the operation and support of SAP. For example, SAP is operated within the existing Health Canada network and relies on the security measures and protection in place. There is no extra protection

against intrusion specifically implemented for SAP; the anti-virus protection implemented for all servers and workstations at HC apply to the SAP system as well.

In addition, the SAP system configuration parameters for password management are set up to be in compliance with Health Canada and central security standards. Health Canada makes use of the enhanced security features of SAP such as: defining the minimum length of a password; defining the number of attempts to use an incorrect password before the account is locked; comparing new passwords against a list of unacceptable passwords; and forcing a 60-day password reset period (where users must re-set their password every 60 days or lose access to the system).

SAP development requests and change requests are managed within FIRMS in a complete manner providing reasonable control – this is discussed more fully in the Change Management section of this report. Patch management is a term describing a process of keeping SAP and its related software and hardware up to date with the latest corrections – including security corrections. Patches normally impact three major areas: operating system, database, and SAP itself. Patches do not follow the standard change management process for security updates. Instead, FIRMS has created specific instructions or "how-to" documents describing step-by-step procedures based on the technical advisory notes from the vendors or the IFMS Cluster for all major patch implementations. While there is currently no formal Patch Management process followed in the unit, there have not been any major changes/patches implemented for the last several years.

Although several "how-to" documents exist that provide some consistency, these documents do not appear to have been formally reviewed and approved. A number of the FIRMS team members are relatively new to the unit – being 6 months to a year in place. As a major upgrade to version 6.0 of the SAP product is expected within the next 12 months, FIRMS had indicated they will build a formal Patch Management process.

In addition to following the Cluster in terms of security and internal control, Health Canada should also assess its environment for security lapses and control weaknesses. The existing Threat-Risk Assessment is out of date. Meanwhile, there have been several other assessments carried out, mostly via evaluations or audits from several different sources. The Office of the Auditor General validates computer controls regularly, and the IFMS Cluster conducted a security health check in 2010. FIRMS has taken corrective measures and responded to audit recommendations in order to mitigate the identified risks. FIRMS has had discussions with IT Security in Health Canada on the requirement to have a formal TRA completed.

Recommendation 3

It is recommended that the Assistant Deputy Minister, Chief Financial Officer Branch, in consultation with the Assistant Deputy Minister, Corporate Services Branch, carry out the formal Threat and Risk Assessment (TRA) for SAP in line with the Health Canada IT Security Policy.

Management Response

Management agrees with this recommendation.

FIRMS and FIRMS-IT will work with CSB to update the Threat and Risk Assessment (TRA) for SAP in line with the Health Canada *IT Security Policy*.

2.3.2 Security Monitoring of SAP

Audit Criterion: *The Department has implemented SAP security monitoring activities in accordance with the guidelines prescribed by the Integrated Financial and Material System (IFMS).*

System security within the SAP product is a combination of system features and imposed environmental controls. SAP is a very large, complex product that requires many decisions during implementation to make use of system features. This process of making specific decisions is called "configuration" rather than development or maintenance. How the SAP settings are configured will have an impact on what security is operational within the product. Health Canada follows the Government of Canada lead in the implementation of security features and related controls.

A business critical application like SAP requires continuous monitoring of its security features. What a user can do in SAP is controlled by his or her role identified in SAP as a profile. A key concern is that mutually exclusive roles cannot be assigned to a single user – that is, segregation of duties is maintained. As almost anything can be configured into SAP: monitoring of the SAP user roles, authorizations created/changed, detailed user's actions and segregation of duties should be a regular and formal process. FIRMS has a security team whose role it is to monitor security concerns within the SAP operation.

FIRMS has adapted a SAP security monitoring program, as well as documented and implemented SAP security monitoring activities in accordance with the guidelines provided by the Integrated Financial and Material System (IFMS) Cluster. This procedure consists of more than twenty steps which are to be executed either manually or automatically following a weekly, monthly, or semi-annual pattern.

In SAP, a significant amount of data is placed into tables. Critical user authorizations are defined in such a table and are considered a high risk to Health Canada. Accordingly, the table involved should be maintained and safeguarded appropriately by having a clear segregation of duties among the Security team roles. There is such a segregation of duties between the individual who maintains this table (Security Team Lead) and the individual who runs the segregation of duties monitoring reports (Security Administrator).

The FIRMS Client Support team is responsible for receiving user inquiries, requests, and trouble reports concerning the FIRMS/SAP operation through the operation of a local "help desk". Help desk procedural documentation provides clear guidance to accurately

resolve or properly escalate issues as appropriate. All calls to the National Service Desk reporting a problem/issue or request for information are entered into the Department's service desk software tool. Service desk tickets related to SAP operations are referred to the FIRMS/SAP Help Desk. Other sources of reported issues include emails, phone calls and even walk-in requests. Of the sample of ten security-related calls reviewed, all were fully documented including incident Type/Category/Ranking, descriptions, impacts, actions, status, change history, etc. Most SAP-related incidents concern individuals' passwords.

One key aspect of monitoring user roles is to test changes for segregation of duties impacts. Health Canada uses a tool provided by the IFMS Cluster to monitor for potential conflicts in segregation of duties within SAP every time a change in authorization for a user is requested. The FIRMS Client Support Team is responsible for running the Segregation of Duties test tool and, if needed, following with requests for review by the Security Team lead, and / or initiating the appropriate sign-off by the requesting manager. This tool is also part of the semi-annual monitoring activity. [Exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b)]

[Exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b)]

Recommendation 4

It is recommended that the Assistant Deputy Minister, Chief Financial Officer Branch, enhance SAP security monitoring to detect and address conflicts in the segregation of duties.

Management Response

Management agrees with this recommendation.

FIRMS will review and address the two specific combinations of transactions the audit highlighted as potential conflicts in the segregation of duties. In addition, FIRMS will share this observation with the IFMS Program office to assess potential enhancements to the current monitoring tool and to identify other monitoring best practices performed by other SAP departments that could be adopted by Health Canada.

3. Conclusion

SAP, as an enterprise financial and material management business solution for the Government of Canada, has significant support both within Health Canada and across the government community. The control environment for SAP management and operation within the Department is clearly evident and shows evidence of following the IFMS Cluster. Within that control environment, a separate organizational unit exists with the specific mandate of managing the SAP operation – roles and responsibilities are defined and employees are aware of their accountability. A collaborative partnership between business and information technology teams has developed to address SAP operation in an integrated manner.

Individual control areas reviewed are functioning. For example, management of change follows a specific process, and general control over user accounts functions well. Procedures directly related to SAP operations have been defined and designed to effectively manage and monitor scheduled processes and ensure the accuracy of data processing activities. There are, however, areas where improvements can be made to strengthen control and reduce operational and security risk.

SAP changes are managed as a process on both FIRMS business teams and on the FIRMS-IT team. While the FIRMS group has previously implemented significant SAP changes, going forward they would benefit from improving the change management process to accommodate large SAP changes as well as the day to day maintenance. This should also capture existing corporate knowledge in the event of the loss of experienced resources.

While overall the control for user accounts is functioning well, FIRMS would benefit from strengthening the area of granting special access privileges and aligning user account expiration dates for temporary users with term or contract end dates. The overall batch control framework ensures the integrity and authenticity of external application data processed by SAP. However, there is a segregation of duties concern between SAP online and batch transaction processing, and the control over incoming batches can be strengthened to better protect SAP data.

Security in the SAP operation is managed following the direction of the IFMS Cluster. Nonetheless, the existing Threat-Risk Assessment (TRA) is out of date and should be re-visited. In addition, tests of segregation of duties conflicts should be strengthened. FIRMS has set up a security monitoring program following the advice and tool set of the IFMS Cluster group. [Exempted pursuant to sections 16(2)(c), 21(1)(a), 21(1)(b)]

Overall, the management control framework for SAP operations exists and is functioning well. There are specific actions that can be taken to further strengthen the framework in addressing the four recommendations.

Appendix A – Lines of Enquiry and Criteria

Audit of SAP General Controls Criteria	
Criteria Title	**Audit Criteria**
Governance and Oversight	
1.1 Oversight	An appropriate governance body (steering committee) has been established to prioritize IT investments for the SAP operation and supporting infrastructure.
1.2 Roles and Responsibilities	Roles and responsibilities related to SAP systems have been clearly defined, documented and understood.
1.3 Monitoring and Management Reporting	Management has established regular monitoring specific to the SAP operation.
System Change Management and Operational Controls	
2.1 Change Management	Documentation exists to support approval by a delegated authority for all software development and changes.
2.2 User Account Management	User account and role privileges are authorized by a delegated authority and audit trail records are retained.
2.3. Batch Controls	Batch control procedures and exception processing are implemented effectively to ensure the accuracy, integrity and authenticity of external application data processed by SAP.
2.4. Operational Controls	Procedures related to SAP operations have been defined to effectively manage and monitor scheduled processes to ensure the accuracy of data processing activities.
Security Safeguards	
3.1 Security Set-up	SAP configuration settings, certification and accreditation process, and assessment of environmental vulnerabilities comply with Government of Canada operational security standards and objectives.
3.2. Security Monitoring	The Department has implemented SAP security monitoring activities in accordance with the guidelines prescribed by the Integrated Financial and Material System (IFMS).

Appendix B – Scorecard

The rating and supporting explanation summarize the current status for each audit criterion.

Criterion	Rating	Conclusion
Governance and Oversight		
Oversight	**S**	Oversight provided at the Government of Canada level and departmental level.
Roles and Responsibilities	**S**	Roles and responsibilities are clearly defined and understood.
Monitoring and Management Reporting	**S**	Monitoring and reporting occurring as expected.
System Change Management and Operational Controls		
Change Management	**S**	Change management process in place and functioning however better documentation required.
User Account Management	**NMiI**	Special access and expiration dates for term and contract staff could be better managed.
Batch Controls	**NI**	Batch controls should be changed to address segregation of duties issues between the feeder systems and SAP.
Operational Controls	**S**	Procedures relating to operations have been defined and effectively designed.
Security Safeguards		
Security Set Up	**NMiI**	Threat and risk assessment for SAP should be conducted.
Security Monitoring	**NMoI**	Security monitoring should be enhanced to better detect and address conflicts related to the segregation of duties.

S	NMiI	NMoI	NI	U	UCBM
Satisfactory	Needs Minor Improvement	Needs Moderate Improvement	Needs Improvement	Unsatisfactory	Unknown; Cannot Be Measured

Appendix C– SAP Batch Interface Files

[Sensitive security-related information consistent with the exemption provisions of the *Access to Information Act* removed.]