Canadian Heritage Patrimoine canadien

Canada

Audit of Policy on Internal Control – Information Technology General Controls (ITGCs) Audit

Office of the Chief Audit Executive
Audit and Assurance Services Directorate

March 2015

Cette publication est également disponible en français.

This publication is available in accessible PDF format
on the Internet at http://www.pch.gc.ca

Catalogue No. CH6-31/2015E-PDF
ISBN: 978-0-660-02111-9

Table of Contents

Executive Summary

Introduction

The Treasury Board Secretariat introduced the Policy on Internal Control in 2008, with an effective date of April 1, 2009. The objective of the Policy is that risks relating to the stewardship of public resources be adequately managed through effective and efficient internal controls within departments and across the government. The Policy on Internal Controls supports the fundamental principles of the Financial Administration Act (FAA), which is the cornerstone of the legal framework for general financial management and accountability of federal government organizations and Crown corporations.

Given the continued reliance on information systems and financial controls, adequately designed and operating IT General Controls (ITGCs) are necessary to properly support Internal Control over Financial Reporting. Appropriate controls related to ITGCs are fundamental in determining whether reliance can be placed on automated business process controls that support significant accounts presented in the financial statements.

The authority for this audit is derived from the Multi-Year Risk-Based Audit Plan 2014-2015 to 2016-2017 which was recommended by the Departmental Audit Committee and approved by the Deputy Minister in June 2014.

The objective of this audit engagement was to provide assurance that ITGCs, as part of internal control over financial reporting and overall stewardship of IT assets, are clearly established and utilized to support the Department in meeting its mandate and objectives, particularly through the support provided by ITGC's to the effective operation of application controls, including controls over input, processing and output.

The scope of this audit included ITGCs related to the following four control areas:

1. Logical security over access to application programs and data;
2. Program changes to applications, including patching or versioning;
3. Program development activities (although it was confirmed that there were no such activities in the current period); and
4. Operational activities, including job scheduling, problem management, back-ups.

The above control areas were in scope only as they related to the applications supporting internal control over financial reporting. As part of the planning phase, these applications were identified as the following:

- SAP – the PCH financial system of record.
- AAPMIS – Athlete Assistance Program Management Information System. This system manages the assistance payments to amateur athletes.
- RPS – Regional Pay System. This is in scope only as it relates to management of PCH users with access to RPS, as all other aspects of ITGCs are the responsibility of Public Works and Government Services Canada, who provide the application to departments.

The period covered by this audit is the current fiscal year, from April 1, 2014 to the completion of the audit fieldwork in December 2014.

Key Findings

Testing was performed for each in-scope application and each control area as it was applicable to each in-scope application. Throughout the audit, the audit team observed many strong control areas in management of ITGCs, as well as some areas where control activities should be strengthened. The overall results of testing have been summarized in the table below:

		SAP	AAPMIS	RPS
Access to Programs/Data	IT Security Policy & Standards	PCH		
	User Authentication	PCH	PCH	PWGSC
	User Access Administration	PCH	PCH	PCH
	User Access Revalidation	PCH	PCH	PCH
	Segregation of Duties between requesting and granting access	PCH	PCH	PCH
Program Changes	Policy & Procedures	PCH	PCH	PWGSC
	Specification and Tracking of Change Requests	PCH and AAFC	PCH	PWGSC
	Authorization	PCH	PCH	PWGSC
	Testing and Quality Assurance	PCH	PCH	PWGSC
	Promotion to Production	PCH and AAFC	PCH	PWGSC
	Emergency changes	PCH	PCH	PWGSC
Computer Operations	Job Scheduling and Monitoring	PCH	PCH	PWGSC
	Back-up Management	AAFC and SSC	PCH and SSC	PWGSC
	Help Desk/Problem Management	PCH	PCH	PWGSC

Legend	Description
Green	Controls exist and evidence of performance of the control is consistently demonstrated.
Yellow	Controls partially exist and/or some inconsistency observed in performance of the control.
Red	Controls do not exist or significant inconsistency observed in performance of the control.

As is evident from the green cells in the table above, PCH has many strong controls in place in the areas of ITGCs, and these controls were found to be operating effectively over the period of the audit.

Each of the cells highlighted in yellow indicate a finding was noted as a result of testing the relevant ITGC area, either in the design of the control procedures or the consistent operation of the control procedures throughout the period of testing. For each yellow cell, the control findings are set out below.

SAP:

- User access to the SAP system is not consistently being removed on a timely basis when users are terminated or otherwise leave the department.
- A number of monitoring controls over SAP user access are in place but should be enhanced to include:
  - periodic review and reconfirmation of access rights for headquarters users, and
  - more timely completion of existing segregation of duties reviews.
- There is no documented change management policy and procedures in place to guide all stages of processing changes to the SAP application.

AAPMIS:

- Passwords are not changed on a regular basis.
- A segregation of duties conflict exists for one user, who approves changes to access and also has the ability to set up that access in the application.
- There is no documented change management policy and procedures in place to guide all stages of processing changes to the AAPMIS application.
- There is no defined process for tracking and managing problems and incidents occurring for AAPMIS.

Recommendations

SAP:

The Chief Financial Officer should:

1. Review and revise the existing process whereby the SAP security team obtains notification of individuals who are terminated or are otherwise leaving the Department, so that SAP user access can be removed in a timely manner.
2. Enhance the control activities related to user access monitoring in the following areas:
   a) Implement a process for a periodic access revalidation of SAP users at headquarters, and the roles assigned to each, to be conducted at least annually and formally documented. All adjustments to user access required as a result of the revalidation should be promptly processed.
   b) Establish a timeline for completion of segregation of duties reviews performed, including the immediate processing of any identified changes to user access to remove segregation of duties conflicts.
3. Require that a change management directive be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the SAP application.

AAPMIS:

The Executive Director, Sport Excellence should:

4. Implement a procedure to require password changes on a regular basis for all users with access to AAPMIS.
5. Implement a requirement that no user has the ability to both approve requests for access to AAPMIS and grant that access within the application.
6. Require that a size-appropriate change management policy and procedures be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the application.
7. Implement a process whereby application problems/incidents with AAPMIS are tracked, analyzed and their resolution recorded.

Statement of Conformance

In my professional judgment as Chief Audit Executive, the audit conforms with the Internal Auditing Standards for the Government of Canada as supported by the results of the quality assurance and improvement program.

Audit Opinion

In my opinion, the controls over management of IT general controls have various risk areas that require management attention, with low risk exposures related to the overall impact on internal control over financial reporting and stewardship of IT assets.

Signed by

Maria Lapointe-Savoie
Chief Audit Executive
Department of Canadian Heritage

Audit Team Members

Maria Lapointe-Savoie - Director
Dylan Edgar – Audit Manager
Jean-Phillipe Rioux – Auditor
With the assistance of external resources

1. Introduction and Context

1.1 Authority for the Project

The authority for this audit is derived from the Multi-Year Risk-Based Audit Plan 2014-2015 to 2016-2017 which was recommended by the Departmental Audit Committee (DAC) and approved by the Deputy Minister in June 2014.

1.2 Background

As an institution of the Government of Canada, Department of Canadian Heritage (PCH) is required to manage the domain of IT General Controls (ITGCs) in a manner that supports the government's overall objectives and the delivery of information and services to Canadians. These requirements are formally set out in government-wide legislation, policies and standards.

The Treasury Board Secretariat introduced the Policy on Internal Control in 2008, with an effective date of April 1, 2009. The objective of the Policy was that risks relating to the stewardship of public resources be adequately managed through effective and efficient internal controls within departments and across the government.

The key expected results of the Policy on Internal Control were that:

- Effective risk-based systems of internal control be in place in departments that are properly maintained, including on-going monitoring, periodic assessments and timely corrective measures when issues are identified;
- Effective systems of internal control over financial reporting operate in departments as demonstrated by the departmental Statement of Management Responsibility Including Internal Control Over Financial Reporting (which was phased in over a three year period); and
- Stakeholders at all levels be aware of and have a clear understanding of their roles, responsibilities, and accountabilities with respect to internal controls.

The Policy on Internal Control supports the fundamental principles of the Financial Administration Act (FAA), which is the cornerstone of the legal framework for general financial management and accountability of federal government organizations and Crown corporations.

Given the continued reliance on information systems and financial controls, adequately designed and operating IT General Controls are necessary to properly support Internal Control over Financial Reporting (ICFR). Appropriate controls related to ITGCs are fundamental in determining whether reliance can be placed on automated business process controls that support significant accounts presented in the financial statements.

2. Objective

The objective of this audit engagement was to provide assurance that ITGCs, as part of internal control over financial reporting and overall stewardship of IT assets, are clearly established and utilized to support the Department in meeting its mandate and objectives, particularly through the support provided by ITGC's to the effective operation of application controls, including controls over input, processing and output.

3. Scope

The scope of this audit included ITGCs related to the following four control areas:

1. Logical security over access to application programs and data;
2. Program changes to applications, including patching or versioning;
3. Program development activities, including data conversions; and
4. Operational activities, including job scheduling, problem management, back-ups.

The above control areas were in scope only as they related to the applications supporting ICFR. As part of the planning phase, these applications were identified as the following:

- ➢ SAP – the PCH financial system of record. The PCH instance of SAP is managed by PCH staff and hosted by Agriculture and Agrifood Canada (AAFC) who, per the Memorandum of Understanding, provide some SAP technical support as well as database support. Parks Canada shares the same SAP instance as PCH and the PCH SAP team administer SAP on behalf of Parks Canada.
- ➢ AAPMIS – Athlete Assistance Program Management Information System. This system manages the assistance payments to amateur athletes. It is a smaller application with a limited number of users, managed internally by PCH.
- ➢ RPS – Regional Pay System. This is in scope only as it relates to management of PCH users with access to RPS, as all other aspects of ITGCs are the responsibility of Public Works and Government Services Canada, who provide the application to departments.

In addition, control areas were included only as they relate to controls exercised by PCH, and excluded any controls that are the responsibility of another government department. There are two other government departments that are responsible for portions of the ITGC control environment at PCH – Shared Services Canada (SSC) and AAFC. The ITGC approach for each was as follows:

- SSC – owns the infrastructure, which includes the data centers, the hardware and the systems software. Consistent with the approach adopted across the federal government, this audit fully excluded any SSC controls. SSC has recognized their control responsibility and has committed to complete testing of their ITGCs and to provide results to departments, as outlined in an e-mail from SSC to departments on May 30, 2014.
- AAFC – provides the hosting environment for the SAP application. Responsibilities of AAFC and PCH are set out in a Memorandum of Understanding. The audit team attempted to obtain from AAFC any separate testing performed and the results from

that testing for the ITGC components they provide to PCH, but AAFC advised they do not have any separate reporting available for PCH. As a result, AAFC was contacted directly during this audit to respond to specific inquires in the areas of controls over database support and management of back-ups. The responses received have been used as evidence for this audit, although it is to be noted that these areas have not been independently tested as part of this audit.

A summary of each of the in-scope control areas, by application environment, is included in the table below. Only the areas shaded in grey were tested for each application environment.

		SAP	AAPMIS	RPS
Access to Programs/Data	IT Security Policy & Standards	PCH	PCH	N/A
	User Authentication	PCH	PCH	PWGSC
	User Access Administration	PCH	PCH	PCH
	User Access Revalidation	PCH	PCH	PCH
	Segregation of duties between requesting and granting access	PCH	PCH	PWGSC
	Database Security	AAFC	PCH	PWGSC
	Operating System Security	SSC	SSC	SSC
Program Changes	Policy & Procedures	PCH	PCH	PWGSC
	Specification, Authorization, and Tracking of Change Requests	PCH and AAFC	PCH	PWGSC
	Testing and Quality Assurance	PCH	PCH	PWGSC
	Promotion to Production	PCH	PCH	PWGSC
	Emergency changes	PCH and AAFC	PCH	PWGSC
Program Development	Management of Development and Implementation Activities	Not applicable at this time as no significant development in 2014/2015.	Not applicable at this time as no significant development in 2014/2015.	PWGSC
	Project Initiation, Analysis, and Design			PWGSC
	Construction/Package Selection			PWGSC
	Testing and Quality Assurance			PWGSC
	Data Conversion			PWGSC
	Implementation in Production			PWGSC
Computer Operations	Job Scheduling and Monitoring	PCH	PCH	PWGSC
	Back-up Management	AAFC and SSC	PCH and SSC	PWGSC
	Help Desk/Problem Management	PCH	PCH	PWGSC

The period covered by this audit is the current fiscal year, from April 1, 2014 to the completion of the audit fieldwork in December 2014.

4. Approach and Methodology

All audit work was conducted in accordance with the Treasury Board Secretariat's *Internal Auditing Standards for the Government of Canada*, and *Policy on Internal Audit* and the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing.*

Audit criteria identify the standards against which an assessment is made and form the basis for the audit work plan and conduct of the audit. Audit criteria are specific to each audit's objectives and scope. The detailed audit criteria for the audit objectives for the ITGC Audit are provided in Appendix A. Audit criteria were developed based on *'Control Objectives for Information Technology' (COBIT),* a widely-accepted international publication setting out good practices for IT governance and management. The COBIT framework has been used by many federal government departments in scoping and testing their ITGCs in support of internal control over financial reporting.

The audit methodology included, but was not limited to:

- A review of the Department's documentation, guidelines and procedures, policies and relevant legislation;
- An analysis of various other documentation and reports, including system reports or viewing of system configuration settings on screen, accompanied by knowledgeable PCH system administrators;
- A collection of data through interviews and observations with the Department's personnel to examine processes, procedures and practices;
- Testing of a selection of transactions for the period from April 1, 2014 to the completion of the audit fieldwork to determine whether the ITGC key controls for each in-scope application were operating effectively throughout the period.

The audit was conducted from the National Capital Region with minor regional involvement, since it was determined during the planning phase that the ITGCs for the in-scope applications are administered by the system support teams based in the National Capital Region.

5. Observations and Recommendations

This section presents detailed findings and related recommendations for the ITGC Audit. The findings are based on a combination of the evidence gathered through the examination of documentation, analysis, transaction and file testing, and interviews conducted for each of the audit criterion. Appendix A provides a summary of all findings and conclusions for each of the criteria assessed by the audit team. During the course of the audit, minor findings were communicated directly to management.

An overview of the results of testing is evident from the summary control matrix below.

		SAP	AAPMIS	RPS
Access to Programs/Data	IT Security Policy & Standards	🟩 PCH		
	User Authentication	🟩 PCH	🟨 PCH	PWGSC
	User Access Administration	🟨 PCH	🟩 PCH	🟩 PCH
	User Access Revalidation	🟨 PCH	🟩 PCH	🟩 PCH
	Segregation of Duties between requesting and granting access	🟩 PCH	🟨 PCH	🟩 PCH
Program Changes	Policy & Procedures	🟨 PCH	🟨 PCH	PWGSC
	Specification and Tracking of Change Requests	🟩 PCH and AAFC	🟩 PCH	PWGSC
	Authorization	🟩 PCH	🟩 PCH	PWGSC
	Testing and Quality Assurance	🟩 PCH	🟩 PCH	PWGSC
	Promotion to Production	🟩 PCH and AAFC	🟩 PCH	PWGSC
	Emergency changes	🟩 PCH	🟩 PCH	PWGSC
Computer Operations	Job Scheduling and Monitoring	🟩 PCH	🟩 PCH	PWGSC
	Back-up Management	AAFC and SSC	🟩 PCH and SSC	PWGSC
	Help Desk/Problem Management	🟩 PCH	🟨 PCH	PWGSC

The legend for the matrix is as follows:

Evaluation	Description
Green	Controls exist and evidence of performance of the control is consistently demonstrated.
Yellow	Controls partially exist and/or some inconsistency observed in performance of the control.
Red	Controls do not exist or significant inconsistency observed in performance of the control.

As is evident from the green cells in the table above, PCH has many strong controls in place in the areas of ITGCs, and these controls were found to be operating effectively over the period of the audit.

Each of the cells highlighted in yellow indicate a finding was noted as a result of testing the relevant ITGC area, either in the design of the control procedures or the consistent operation of the control procedures throughout the period of testing. For each yellow cell, the details of the findings are set out below. Findings are presented by application and then by control area within the application.

5.1 *SAP*

5.1.1 User Access Administration

User access to the SAP system is not consistently being removed on a timely basis when users are terminated or otherwise leave the department.

Control criteria:

Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.

Observations

The SAP security team follows defined procedures for managing user access to SAP, including procedures to add, modify and remove user access. The procedures to add and modify user access were tested and no exceptions were noted. To test the timeliness of access removals, reports of terminated users were obtained directly from Human Resources as well as reports from the ticketing system that tracks requests for access changes, and the dates of termination from these reports were compared to the dates the user access was actually removed in SAP. Based on this testing, the following was noted:

- There were five departed users with end dates ranging from May to September 2014 who still had active SAP accounts as at November 26, 2014, which is the date the testing was completed; and
- For those users tested whose SAP access had been removed, access for 11 of 34 departed users was not removed in a timely manner. For these 11 departed users, SAP access was removed between 9 and 211 days after the user's termination date.

The ability to access the SAP system first requires network sign-on and then sign-on to the SAP application, thus providing two levels of access control. If the user access termination procedure at the network level results in timely removal of user accounts at that level, the risk from delays in removal of access to SAP is eliminated. We were unable to test timeliness of removal of network access as the date of removal is not evident on each network account. However, in addition to procedures around network access removal, each application team also has responsibility to ensure access remains current for all users

Risk Assessment

Failure to remove access to SAP on a timely basis for users who no longer require it can result in unauthorized access to the SAP application. In addition, this is in violation of the Department's 'Identification and Authentication Standard' section 5.2 which states that 'users will have access to only that information required for their job function and clearance level.'

Recommendation #1

The Chief Financial Officer should:

Review and revise the existing process whereby the SAP security team obtains notification of individuals who are terminated or are otherwise leaving the Department, so that SAP user access can be removed in a timely manner.

5.1.2 User Access Revalidation

A number of monitoring controls over SAP user access are in place but should be enhanced to include:

- periodic review and reconfirmation of access rights for headquarters users, and
- more timely completion of existing segregation of duties reviews.

Control criteria:

A control process exists and is followed to periodically review and confirm access rights, including the disabling of inactive user accounts.

Observations

The SAP security team performs a number of security monitoring activities that are completed either on a weekly, monthly, quarterly or semi-annual basis. A review of these activities indicated that they include many strong control procedures to enhance and maintain the security of the SAP application.

Included in the security monitoring activities is a requirement to send reports of all SAP userIDs to each region on a quarterly basis to re-confirm that those users still require their SAP access. This, however, is not required for headquarters users, although they represent the largest percentage of SAP users.

Another key monitoring activity is the semi-annual review to identify potential segregation of duties conflicts existing with user assignments in the SAP system. The segregation of duties review covers all SAP users regardless of the risk level. However, segregation of duties conflicts lies with the Accounting Operations, Systems and AAFC technical teams. Segregation of duties conflicts identified are assigned to designated individuals to assess and indicate any required modifications, which are then processed by the SAP Systems team. Testing indicated that, although the process is in place, there are delays in completing the reviews. The review based on reports run as of May 26, 2014 was completed as follows:

- Accounting Operations – review completed on July 18th; the requested access change was removed on September 9th.
- Systems – review completed on July 2nd; the requested access change was removed on July 16th.
- AAFC – review completed on June 24th; the requested access change was removed on June 30th.

- Parks – Parks users were included in the May 2014 review, but Parks advised they were unable to complete the review due to other priorities. As Parks is a separate entity, PCH has a responsibility to provide them with the information on high-risk segregation of duties conflicts within their instance of the application, but no responsibility to ensure Parks completes the review.

Risk Assessment

Lack of a process to revalidate SAP user access for headquarters users on a periodic basis increases the risk that inappropriate access may exist for users who have left the Department or who have changed positions and thus have accumulated access that is no longer required to perform their job responsibilities.

Delays in review of potential segregation of duties conflicts with user access, and delays in removing these conflicts when they are identified for removal, could result in unauthorized transaction processing in SAP and thus inaccurate financial results.

Recommendation #2

The Chief Financial Officer should:

Enhance the control activities related to user access monitoring in the following areas:

a) Implement a process for a periodic access revalidation of SAP users at headquarters, and the roles assigned to each, to be conducted at least annually and formally documented. All adjustments to user access required as a result of the revalidation should be promptly processed.

b) Establish a timeline for completion of segregation of duties reviews performed, including the immediate processing of any identified changes to user access to remove segregation of duties conflicts.

5.1.3 Change Management Policy and Procedures

There is no documented change management policy and procedures in place to guide all stages of processing changes to the SAP application.

Control criteria:

A Change Management Policy and related procedures exist, have been approved by an appropriate level of management, and are communicated to impacted staff.

Observations

Although the SAP Systems team was able to describe the process followed to manage a change to the SAP application, there is no approved documented change management policy and procedures in place to guide all stages of processing changes to the SAP application. There is a ‘STAR System Change Management Practices’ document dated March 16, 2010; however, this document is more than four years old and is still in draft with sections that are incomplete. Additionally, the change management team indicated this is not current and is not completely followed. Good industry practices indicate that such a document should address, at a minimum, the key steps in the change management process and the checkpoints and approvals required, including requirements in the following areas:

- documentation of requests for changes
- requests for changes are authorized by an appropriate level of management
- changes are fully tested, validated and approved prior to being placed in production
- restrictions exist over access for migrating changes into the production environment.

Risk Assessment

The lack of a formal documented change management directive increases the risk that activities performed to process program changes may be inadequate and/or inconsistently followed, with the result that processing errors may be introduced into the production environment.

In addition, as this is a departmental application resulting in financial transactions, lack of formalization of procedures creates a risk to the Department in the event of staff turnover.

Recommendation #3

The Chief Financial Officer should:

Require that a change management directive be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the application.

5.2 *AAPMIS*

5.2.1 User Authentication

Passwords are not changed on a regular basis.

Control criteria:

Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.

Observations

Access to the AAPMIS application is via a unique username and password. When new users are set up, a password is selected to meet length and complexity requirements and is set up by the database team. There is currently no feature in the AAPMIS application or established at the database level to require that passwords be changed on a regular basis, or to allow users to change their own password within the application. The result is that user passwords can go unchanged for an extended period. In accordance with departmental requirements as set out in the ‘Identification and Authentication Standard’, passwords must be changed at least every six months, be at least eight characters in length and follow certain composition requirements.

Password change should be enforced by the application. However, as this may not be practical for AAPMIS, and since the number of AAPMIS users is small, a manual procedure could be implemented whereby the AAPMIS team schedules the password changes and enforces a manual process for all AAPMIS users to communicate with the application database administrator every six months to process the requested changes.

Risk Assessment

Failure to change passwords to applications on a regular basis increases the risk that passwords will become known to others and result in potential unauthorized access to the application.

Recommendation #4

The Executive Director, Sport Excellence should:

Implement a procedure to require password changes on a regular basis for all users with access to AAPMIS.

5.2.2 Segregation of Duties Between Requesting and Granting Access to AAPMIS

A segregation of duties conflict exists for one user, who approves changes to access and also has the ability to set up that access in the application.

Control Criteria:

Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed

Observations

Due to the small number of users with access to AAPMIS, the process to grant or modify user access is informal, consisting of an e-mail from the Program Analyst setting out the request for change, which is approved by the Manager, and then provided to the database team to set up the access. A review of users with access to set up or modify access at the database level however, revealed that the Manager also has this access through membership in the ‘admin’ group, although we were advised he never uses it. Having responsibility to both approve requests for access and the ability to process those requests creates a segregation of duties conflict.

Risk Assessment

Maintaining appropriate segregation of duties is important so that no individual can process a transaction from end to end. In this case, inappropriate access could be granted to the AAPMIS application with the risk of unauthorized processing of transactions.

Recommendation #5

The Executive Director, Sport Excellence should:

Implement a requirement that no user has the ability to both approve requests for access to AAPMIS and grant that access within the application. For the one user who currently has the ability to perform both, the ability to grant the access should be re-assigned to another member of the team to eliminate the conflict.

5.2.3 Change Management Policy and Procedures

There is no documented change management policy and procedures in place to guide all stages of processing changes to the AAPMIS application.

Control criteria:

A Change Management Policy and related procedures exist, have been approved by an appropriate level of management, and are communicated to impacted staff.

Observations

Although the number of program changes made to AAPMIS is small, there is no documented change management policy and procedures in place to guide all stages of processing changes to the application. Application changes are programmed by an external consultant. However, the procedures for providing instructions to the consultant and requirements for AAPMIS team testing and approvals rely on the knowledge and experience of long-time staff. Good industry practices indicate that such a document should address, at a minimum, the key steps in the change management process and the checkpoints and approvals required, including guidance in the following areas:

- requirements for documentation of requests for changes
- requests for changes are authorized by an appropriate level of management
- changes are fully tested, validated and approved prior to being placed in production
- restrictions exist over access for migrating changes into the production environment.

Risk Assessment

Although the number of program changes for AAPMIS has been low, deficiencies in change management could significantly impact the integrity of the application. In addition, as this is a departmental application resulting in financial transactions, lack of formalization of procedures creates a risk to the Department in the event of staff turnover.

Recommendation #6

The Executive Director, Sport Excellence should:

Require that a size-appropriate change management policy and procedures be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the application.

5.2.4 Problem Management

There is no defined process for tracking and managing problems and incidents occurring for AAPMIS.

Control criteria:

A problem management system has been defined and implemented to provide that operational events that are not part of standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner.

Observations

As part of the audit, the team planned to test whether problems or incidents relating to AAPMIS were analyzed and resolved in a timely manner, but was unable to obtain a listing of any such incidents occurring in the fiscal year. Although the audit team was advised that there are few problems/incidents related to AAPMIS, there is no ticketing system or other process in place for tracking AAPMIS incidents and their ultimate resolution. Ideally problems and incidents would be tracked in a ticketing system; however, due to the reported small number of incidents with AAPMIS, this could be achieved through tracking via excel or other means that is stored in a location available to all AAPMIS team members as required.

Risk Assessment

Failure to track application incidents can result in any of the following:

- unresolved incidents that continue to cause system issues
- lack of a record of previous incidents and their resolution to provide documentation of the resolution in case of re-occurrence of the incident
- lack of knowledge in case of staff turnover.

Recommendation #7

The Executive Director, Sport Excellence should:

Implement a process whereby application problems/incidents with AAPMIS are tracked, analyzed and their resolution recorded. Ideally problems and incidents would be tracked in a ticketing system; however, due to the reported small number of incidents with AAPMIS, this could be achieved through tracking via excel or other means that is stored in a location available to all AAPMIS team members as required.

Appendix A – Audit Criteria

The conclusions reached for each of the audit criteria used in the audit were developed according to the following definitions.

Numerical Categorization	Conclusion on Audit Criteria	Definition of Conclusion
1	Well Controlled	• well managed, no material weaknesses noted; and • effective.
2	Controlled	• well managed, but minor improvements are needed; and • effective.
3	Moderate Issues	Has moderate issues requiring management focus (at least one of the following two criteria need to be met): • control weaknesses, but exposure is limited because likelihood of risk occurring is not high; • control weaknesses, but exposure is limited because impact of the risk is not high.
4	Significant Improvements Required	Requires significant improvements (at least one of the following three criteria need to be met): • financial adjustments material to line item or area or to the department; or • control deficiencies represent serious exposure; or • major deficiencies in overall control structure. Note: Every audit criteria that is categorized as a **"4"** must be immediately disclosed to the CAE and the subjects matter's Director General or higher level for corrective action.

The following are the audit criteria and examples of key evidence and/or observations noted which were analyzed and against which conclusions were drawn.

Audit Sub-Objective #1: Access to Programs and Data: Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to safeguard information against unauthorized use, disclosure, modification, or loss of data.				
Criteria #	**Audit Criteria**	**Conclusion**		**Examples of Key Evidence / Observation**
		SAP	**AAPMIS**	
1.1	An information security policy and related standards exist, have been approved by an appropriate level of management, and are communicated to impacted staff.	2		• IT Security Policy, Directive, Framework and supporting Standards are in place and are available to users through the intranet. • All of the above were last reviewed in 2010. The IT Security Policy states in section 1.3 that “This IT Security Policy will be reviewed, at a minimum, every 3 years thereafter, and updated if required”. Based on the above, these documents are overdue for review and any required updating.
1.2	Procedures exist and are followed to authenticate all users to the system to support the validity of transactions.	1	2	• All applications require unique user IDs and user profiles to manage access. • Privileged user access has been appropriately restricted to administrators. • Strong password usage is enforced for SAP. For AAPMIS, the system does not enforce password changes. • Audit trails are available to enable follow-up on transactions.

Criteria	Audit Criteria	Conclusion		Examples of Key Evidence / Observation
		SAP	AAPMIS	

1.3	Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending and closing user accounts.	3	AAPMIS = 1
			RPS = 1
				• Procedures have been established to add and modify user access and require manager approval.
				• For SAP, although procedures are in place to remove user access, it was found not to be operating effectively to remove access in a timely manner.
				• For AAPMIS and RPS, small user groups enable closer overall management of user changes.

1.4	A control process exists and is followed to periodically review and confirm access rights, including the disabling of inactive user accounts.	2	AAPMIS = 1
			RPS = 2
				• For SAP, a user access revalidation is performed on a semi-annual basis for users in the regions but is not performed for users at headquarters, which represent the largest group of users. Partial compensating controls are as follows:
				- on a quarterly basis, all inactive accounts are reported, investigated, and access removed as required.
				- on a semi-annual basis, an SoD analysis is run for key financial transactions and reviewed by Accounting Operations, Systems and AAFC, although it was noted that this is not completed on a timely basis.
				• For AAPMIS, due to the fact that there are only 9 user accounts on the application, all access is reviewed each time an access change is processed.
				• For RPS, a user access revalidation is not performed on a regular basis. One performed at our request resulted in 3 users whose access should have been removed.

1.5	Controls relating to appropriate segregation of duties over requesting and granting access to systems and data exist and are followed.	1	AAPMIS = 2
			RPS = 1
				• For SAP, user managers must request access while only members of the SAP Systems team can grant access.
				• For AAPMIS, an SoD issue was noted regarding the Manager, who approves all access and also has access to the admin database group, so could set up the access, although the audit team was

				advised this account is never used. • For RPS, PCH can only request access changes. The ability to process access changes in RPS is restricted to PWGSC.

Audit Sub-Objective #2: **Application Change Management:** Controls provide reasonable assurance that changes to applications are authorized, tested, documented and approved prior to implementation in production.

Criteria	Audit Criteria	Conclusion		Examples of Key Evidence / Observation
#		SAP	AAPMIS	
2.1	A Change Management Policy and related procedures exist, have been approved by an appropriate level of management, and are communicated to impacted staff.	3	3	• For SAP, although the SAP systems team were able to describe the procedures followed to manage changes, and no exceptions were noted from our testing of controls under 2.2 to 2.6, the change management policy and procedures have not been documented. • For AAPMIS there are very few changes annually – 1 in 2014 – and changes are programmed by an external consultant. However, the change management procedures have not been documented, and they rely heavily on two long-serving employees to manage all aspects of program changes.
2.2	Requests for program changes, system configuration changes and maintenance (including changes to system software) are standardized, documented and subject to change management procedures.	1	1	• For SAP, a selection of changes were tested and no exceptions were noted. • For AAPMIS, the one change in 2014 was tested and no exceptions were noted.
2.3	Changes to the systems/ applications providing control over financial reporting are authorized by an appropriate level of management.	1	1	• For SAP, a selection of changes were tested and no exceptions were noted. • For AAPMIS, the one change in 2014 was tested and no exceptions were noted.

2.4	Changes to applications and systems are tested, validated and approved prior to being placed into production.	1	1	• For SAP, a selection of changes were tested and no exceptions were noted. • For AAPMIS, the one change in 2014 was tested and no exceptions were noted.
2.5	Controls are in place to restrict access for migrating changes into the production environment.	1	1	• For SAP, system lists of users with access to transport changes to production were obtained and access confirmed to be appropriately restricted. • For AAPMIS, access to migrate changes to production is restricted to two members of the database team.
2.6	Emergency changes to applications and configuration are documented and subject to formal change management procedures.	1	1	• For both SAP and AAPMIS, emergency changes are rare since neither application has 24/7 availability. • For SAP, a review of the change register and inquiry of the SAP systems team indicated no emergency changes in 2014. • For AAPMIS, the one change during the year was not an emergency change.

Audit Sub-Objective #3: **Computer Operations:** Controls provide reasonable assurance that IT support functions are performed regularly and in an orderly fashion.

Criteria #	Audit Criteria	Conclusion		Examples of Key Evidence / Observation
		SAP	AAPMIS	
3.1	Standard procedures for job scheduling and monitoring have been defined and implemented.	1	1	• For SAP, system reports of access to maintain the job schedule and maintain production batch jobs were reviewed and access confirmed to be appropriately restricted to the Basis/Security team. • For SAP, job monitoring is performed on a daily basis through the SM37 screen. The audit team inspected evidence of follow-up of a failed job, as well as a cumulative list of all uncleared failed jobs and determined that failed jobs are being cleared. • For AAPMIS, there is no separate job schedule, as there is only one key job,

				which is the cheque run. This is monitored manually by ensuring a payment report is produced and is accurate, and is manually reconciled to the amount posted to SAP.
3.2	A problem management system has been defined and implemented to provide that operational events that are not part of standard operation (incidents, problems and errors) are recorded, analyzed and resolved in a timely manner.	1	2	• For SAP, problems and incidents are tracked through the Help Desk in Remedy. A selection of SAP incidents were tested and all were found to be analyzed and resolved in a timely manner. • For AAPMIS, although the audit team was advised that there are very few problems/incidents, they are not separately tracked so we were unable to confirm this and recommend that tracking and documentation of the resolution be implemented.
3.3	Management has implemented a strategy for cyclical backup of data and programs, including retention periods and storage.	1 (based on response s provided by AAFC)	1	• For SAP, back-ups are managed by AAFC. Per AAFC responses, they are run daily online and weekly off-line on the weekends, with 4 weeks retention. They are stored off-site weekly (managed by SSC). • For AAPMIS, back-ups are managed by CIOB, and are run daily and weekly. They are stored off-site weekly.
3.4	Back-up logs are monitored for successful completion.	1 (based on response s provided by AAFC)	1	• Per AAFC responses, SAP back-up logs are monitored daily by AAFC using HPDataprotector and with automatic alerts. Per AAFC responses, failed back-ups are monitored daily in accordance with documented procedures. • For AAPMIS, back-up logs are monitored daily by CIOB. Failed back-ups are monitored daily and generally just picked up as part of the following day's back-up.
3.5	Procedures exist and are followed to periodically test the effectiveness of the	1 (based on response	1	• Per AAFC responses, SAP periodic refreshes are performed whenever there is a client request, with the last refresh occurring successfully in January 2015.

	restoration process and the quality of backup media.	s provided by AAFC)		There is also a documented refresh procedure. • For AAPMIS, restore of backup files are tested once a year, or more often when requested by the developers.

Appendix B – Management Action Plan

Audit of Policy on Internal Control – Information Technology General Controls (ITGCs) Audit

5.1 SAP			
Recommendation	**Actions**	**Who**	**Target Date**
1. The Chief Financial Officer should review and revise the existing process whereby the SAP security team obtains notification of individuals who are terminated or are otherwise leaving the Department, so that SAP user access can be removed in a timely manner.	Agree A process to ensure user access is removed in a timely manner when employees who have SAP access depart from the department will be put into place. The inactivation of the financial system access is a secondary control as a departed employee would need building access, active network login and hardware to enter the SAP system. As such this process considered low risk, has previously been done as a periodic work instead of a control step.	Manager, Financial System, FMB	June 2015
Recommendation	**Actions**	**Who**	**Target Date**
2. a) The Chief Financial Officer should implement a process for a periodic access revalidation of SAP users at headquarters, and the roles assigned to each, to be conducted at least annually and formally documented. All adjustments to user access required as a result of the revalidation should be promptly processed.	Agree A process for a periodic access revalidation of SAP users at Headquarters will be put into place.	Manager, Financial System, FMB	December 2015

Recommendation	Actions	Who	Target Date
2. b) The Chief Financial Officer should establish a timeline for completion of segregation of duties reviews performed, including the immediate processing of any identified changes to user access to remove segregation of duties conflicts.	Agree There are enough individuals involved in the payment process to avoid even the most minor overlap of access that could be interpreted as a segregation of duties conflict. Firm timelines will be put in place for future reviews.	Manager, Financial System, FMB	June 2015
Recommendation	**Actions**	**Who**	**Target Date**
3. The Chief Financial Officer should require that a change management directive be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the application.	Agree A formal change management directive will be put in place. This is considered low risk as the not-fully documented process has still ensured appropriate system testing with every change made in SAP.	Manager, Financial System, FMB	June 2015

5.2 AAPMIS

Recommendation	Actions	Who	Target Date
4. The Executive Director, Sport Excellence should implement a procedure to require password changes on a regular basis for all users with access to AAPMIS.	Agree The AAP Unit will request that Chief Information Officer Branch (CIOB) change the randomly generated password for each user every 6 months and notify the user.	Manager, Athlete Assistance Program (AAP)	April 2015

Recommendation	**Actions**	**Who**	**Target Date**
5. The Executive Director, Sport Excellence should implement a requirement that no user has the ability to both approve requests for access to AAPMIS and grant that access within the application. For the one user who currently has the ability to perform both, the ability to grant the access should be re-assigned to another member of the team to eliminate the conflict.	Agree The AAP Unit will request that CIOB remove the ability of the AAP Manager to make access changes to users of AAPMIS. A back up is required for the Program and Policy Analyst, who also has the ability to make access changes to users of AAPMIS.	Program and Policy Analyst, APP	April 2015
Recommendation	**Actions**	**Who**	**Target Date**
6. The Executive Director, Sport Excellence should require that a size-appropriate change management polcy and procedures be documented, approved and implemented to guide the consistent application of procedures for managing changes made to the application.	Agree A size-appropriate change management policy and procedures will be developed for the use by the AAP Unit in managing changes to the AAPMIS.	Manager, AAP	September 2015
Recommendation	**Actions**	**Who**	**Target Date**
7. The Executive Director, Sport Excellence should implement a process whereby application problems/incidents with AAPMIS are tracked, analyzed and their resolution recorded. Ideally, problems and incidents would be tracked in a ticketing system; however, due to the reported small number of incidents with AAPMIS, this could be achieved through tracking via excel or other means that is stored in a location available to all AAPMIS team members as required.	Agree The AAP Unit will develop a system to document and track problems/incidents with AAPMIS from the initial identification of the issue to the resolution of the problem.	Manager, AAP	September 2015