Environment Canada Environnement Canada

# Follow-up Audit of Finance and Corporate Branch's IT Controls over Financial Systems

**June 16 2011**

Canada

## Key Dates

| | |
|---|---|
| Opening conference (launch memo) | June 2010 |
| Audit plan sent to management | Sept 2010 |
| Closing conference (exit debrief) | April 2011 |
| Audit report sent to management | May 2011 |
| Management's response received | May 2011 |
| Penultimate draft report approved by CAE | May 2011 |
| Audit committee recommendation | June 2011 |
| Deputy Minister's approval | January 2012 |

**Prepared by the Audit and Evaluation Team**

## Acknowledgments

The audit team, comprising staff from Ernst & Young, Audit Services Canada and Internal Audit under the direction of Jean Leclerc and Claude Bélisle, would like to thank everyone who contributed to this project and, in particular, those employees who provided insights and comments.

# Table of Contents

# EXECUTIVE SUMMARY

This audit was included in the departmental Risk-Based Audit Plan 2010–2013 as approved by the Deputy Minister, upon the recommendation of the External Audit Advisory Committee.

When the *Federal Accountability Act* was introduced in 2006, it required departments to be able to produce audited financial statements capable of supporting a controls-based audit. This was subsequently changed to a requirement to produce auditable financial statements.

Each department was to conduct a baseline assessment of its capacity to comply with this requirement and to report annually on its progress toward compliance to the Office of the Comptroller General (OCG).

At Environment Canada, this audit readiness assessment was contracted to an outside firm and was conducted in two phases, beginning in 2007. The Phase 2 Report on the Audit Readiness Assessment (March 2009) highlighted a number of issues, including 25 issues in the area of information technology (IT) financial controls. The Department implemented an action plan to remedy the issues identified by the end of March, 2011.

The objective of this audit was to follow up on the action plan in response to the 25 IT financial control issues from the Phase 2 Audit Readiness Assessment report of March 2009, to review their completion and ensure that the control weaknesses identified in that report had been resolved.

### Statement of Assurance

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and the Policy on Internal Audit of the Treasury Board of Canada.

In our professional judgment, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations, as they existed at the time, against the audit criteria.

### Summary of Findings

Since the Phase 2 Audit Readiness Assessment report was released in March 2009, significant effort has been made to address the recommendations and underlying findings regarding the 25 IT financial controls issues. The financial system has undergone major upgrades in its platform and functionality. In particular, in the past 8 months, the Department has migrated the system from a UNIX platform to a LINUX platform, added the asset life-cycle management functionality and patched a number of security threats.

For the work plan arising from the Phase 2 Audit Readiness Assessment of March 2009, which was to be completed by March 2011, we conclude that substantial progress has been made in addressing the 25 IT financial control recommendations. All high-risk areas of control weakness have been mitigated but further work is required to address them fully. Eleven controls were found to be well addressed by the work undertaken to date. Twelve of the remaining controls were found to be largely effective with only minor issues that still need to be addressed—each control posing a low level of risk to the Department. [Text removed to protect the security of the system]

When the audit fieldwork began in earnest in December of 2010, the review team found that almost none of the policy and procedural work had been finished. However, by the time the audit team was able to begin testing, this situation had been largely reversed, with almost all of the policy and procedural work having been completed. This was accomplished in an environment in which the resources of the Finance and Corporate Services Branch were involved in the implementation of the major change in platforms in November 2010, as well as the work involved for the financial year-end.

### Observations and Recommendations

The following is a summary of the observations and recommendations contained in the body of the report.

2.1 Improve sustainability of monitoring controls

The audit team observed that remediation activities had been put in place to address monitoring deficiencies using the existing level of resources. The controls that were implemented will remediate the deficiencies; however, in order for the monitoring to be sustainable over the long term, the automation of certain activities needs to be considered.

Recommendation
The Chief Financial Officer (CFO) should develop a plan for re-engineering the monitoring controls over the financial systems within a continuous improvement strategy in order to integrate them into existing business processes, reduce costs and improve sustainability.

2.2 Work plan required for outstanding items

The audit team observed that residual work remains for the 12 low-level risk controls and the two medium-risk controls.

Recommendation
The CFO should develop a work plan to address the completion of activities outstanding from the work plan arising from the Phase 2 Audit Readiness Assessment report.

2.3 A program of continuous monitoring should be implemented

The recommendations arising from the Phase 2 Audit Readiness Assessment require that many controls be subject to periodic review (monitoring). The audit team found that processes surrounding this monitoring are documented and managed as individual activities, and that the monitoring controls are independently designed and operated.

Recommendation

The CFO should develop a strategy for the continuous monitoring of IT financial controls, which should be part of an overall strategy of monitoring of internal controls.

2.4 Identity and access management controls should leverage information available in human resource systems

The audit team found that many of the controls related to identity and access management, especially those that are detective in nature, would be more effective if the controls could leverage information already available in the HR systems.

Recommendation

The CFO and the Assistant Deputy Minister for HR should establish a strategic plan for leveraging existing user identification for use in the financial systems.

### Management Response

*Agree. Management has developed a management action plan.*

# 1 INTRODUCTION

This audit was included in the departmental Risk-Based Audit Plan 2010–2013 as approved by the Deputy Minister, upon the recommendation of the External Audit Advisory Committee.

Within Environment Canada, the IT controls that support the production of auditable annual financial statements are the responsibility of the Finance and Corporate Services Branch (FCB) and the Chief Financial Officer (CFO).

## *1.1 Background*

When the *Federal Accountability Act* was introduced in 2006, it required departments to be able to produce audited financial statements capable of supporting a controls-based audit. This was subsequently changed to a requirement to produce auditable financial statements.

Each department was to conduct a baseline assessment of its capacity to comply with this requirement and to report annually to the Office of the Comptroller General (OCG) on its progress toward compliance.

At Environment Canada, the audit readiness assessment was contracted to an outside firm (Ernst & Young) and conducted in two phases, beginning in 2007. The Phase 2 Report on the Audit Readiness Assessment (March 2009) highlighted several issues, including 25 in the area of information technology (IT) financial controls. The Department implemented an action plan to remedy the issues identified, by the end of March 2011.

The 25 issues requiring remediation to enable an efficient controls-based audit were in the areas of user access management (i.e. identifying and controlling user access), database account management (i.e. identifying and controlling database privileges), and change management (i.e. documentation and monitoring).

Generally referred to as identity and access management (IAM), these three areas constitute the process of managing which users have access to what information, and how and when they can access it. Amongst other things, effective IAM improves operating efficiency and transparency, along with the effectiveness of key business initiatives. It would be very difficult for any department to conduct a controls-based audit on its auditable financial statements without effective IAM.

## *1.2 Risk Assessment*

In order to scope out the planned audit on the Department’s capacity to conduct a controls-based audit, a preliminary review of background information and a risk assessment highlighted many possible objectives for this engagement. Documentation, including legislation, policies and directives, was reviewed and interviews were conducted with management from the Finance and Corporate Branch and the Chief Information Officer Branch to gain an understanding of the financial control environment and priority requirements, and their impact on Environment Canada.

Specific risks related to the IT financial controls environment were subsequently identified and evaluated as part of the audit planning. Ongoing activities such as the Corporate Accountability and Administrative Renewal (CAAR) project and the planned migration to a newer version of the database management system to support our financial systems were also taken into account.

The CAAR project includes many activities that are meant to address deficiencies identified during the Audit Readiness Assessment. [Text removed to protect the security of the system]

The audit focused on IAM issues in Merlin, the financial system IT application in use at Environment Canada. This approach was taken to avoid duplication of efforts and to add the most value for the Department. The approach took into consideration the results of the Phase 2 Audit Readiness Assessment, which had already focused on IAM issues in many of its IT-related findings, The most effective way of assessing IAM issues in Environment Canada's financial systems, then, was to follow up on the action plan addressing the 25 issues from the Phase 2 Audit Readiness Assessment report.

## 1.3 Objective and Scope

This audit therefore followed up on the Phase 2 Audit Readiness Assessment report of March 2009 by reviewing the completion of the action plan to remedy the 25 IT financial control issues identified in the report, and to ensure that the control weaknesses had been resolved.

The work was carried out in the National Capital Region. Regional involvement was limited to determining whether the controls are implemented in a consistent way across all regions. Further, as the system underwent a major change in platforms in November 2010, testing of IT controls was restricted to those that were operating between the implementation of the new system and March 31, 2011, the end of fiscal year 2010–2011.

## 1.4 Methodology

Audit fieldwork took place between December 2010 and April 2011, using input from two teams. The first team, which was from Audit Services Canada, reviewed through interviews the processes that were proposed as action items as a result of recommendations arising from the Phase 2 Audit Readiness Assessment report. The second team, which was from Ernst & Young, provided assurance by conducting tests of the data and processes, performing a thorough documentation review, and conducting interviews to establish that the recommendations have indeed been implemented and the resulting controls are working as planned. Testing included running scripts to extract information from various IAM-related tables in the application, the database and the operating system, selecting judgemental samples from these extracts and reviewing the files and other related evidence to determine whether the controls had operated effectively.

Although the intent of the timing of the audit work was to be optimized to coincide with the availability of system resources, it became apparent that the resources of the Finance and Corporate Services Branch were involved in the implementation of the major change in platforms in November of 2010 and a major upgrade to test the required controls in February of 2011 (so that they could be implemented in production on April 1, 2011). To further complicate the timing of the audit, Finance and Corporate Services Branch was also busy with the work involved for the financial year-end. This posed a challenge with the audit scheduling and evidence testing. To minimize disruptions to operations at a critical time, the audit team conducted interviews, observations and testing at the same time as the operations staff was performing the implementation testing.

While all of the controls were in place during the audit period, by the time that testing began in April of 2011 there had been insufficient activity to test 11 of the controls. To compensate for the lack of test data, the audit team performed additional review procedures to support the conclusions of this report.

### *1.5 Statement of Assurance*

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and the Policy on Internal Audit of the Treasury Board of Canada.

In our professional judgement, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on a comparison of the situations, as they existed at the time, against the audit criteria.

## 2 FINDINGS AND RECOMMENDATIONS

Findings were based upon evidence collected by Audit Services Canada (ASC), by testing, inquiry and document reviews carried out by Ernst & Young, and by inquiry and document review carried out by staff at Internal Audit.

Since the Phase 2 Audit Readiness Assessment report of March 2009, policy requirements surrounding audited financial statements have been reviewed and changed to auditable financial statements. In addition, Environment Canada’s Financial Statement Audit Readiness (FSAR) project was revisited to allow it to address Corporate Accountability and Administrative Renewal (CAAR) initiatives, with the global objective of improving financial management and accountability. Changes to the organization accompanied these changes in financial management renewal.

Since the audit readiness assessment was finalized in March 2009, Merlin has migrated to a new platform (from UNIX to LINUX), has been patched significantly, and has had its functionality enhanced to include asset life-cycle management.

A major upgrade to Merlin, including improvements to its control environment, was carried out on April 1, 2011. At that time, new account access controls were put in place, including password management controls and improvements to the roles-based (“responsibilities”) access controls. Further, reports necessary for the operation of many of the monitoring controls were also moved into production on that date. The recent implementation of these features meant that there was insufficient time for account-related transactions to occur in order to test the effectiveness of many of the controls that govern these transactions.

The original audit plan was to establish the adequacy of the controls implemented to address the 25 control issues. This was to be based on testing, or on inquiry and document review.

Of the 15 controls that were to be assessed by testing, there was insufficient evidence available to draw assurance-level conclusions for 11. This lack of evidence was largely due to the recent implementation of associated controls. Further audit work will be required to test these controls once sufficient time has passed to allow for transactional evidence to accumulate.

Table 1 – Summary of Primary Audit Work

| Reference to Control Item in Annex 1 | Control Implemented / Risk Level | Primary Audit Work |
|---|---|---|
| 2, 7, 10, 11, 14, 20, 21, 22, 24 | Control implemented | Documentation review |
| 19 | Control implemented | Documentation review (replaced testing) |
| 4 | Control implemented | Control tested |
| 5, 8 | Medium risk | Documentation review & interviews |
| 6 | Low risk | Documentation review & interviews |
| 1, 3, 9, 12, 13, 15, 16, 17, 18 23, 25 | Low risk | Could not test<br>Documentation review & interviews |

In this report, the controls related to the Merlin application were generally considered to pose a higher level of inherent risk than the controls related to the database or to the operating system. As justification for this assignment of risk levels, two factors were considered.

First, the failure of operating system or database controls can have a major short-term impact on the availability of the system and of its information; however, to a large extent, compensating controls such as backups and business resumption planning reduce the impact. In contrast, failures of the application controls can lead to an impact on the confidentiality, integrity and availability of the information in the system, posing a far greater risk to the Department in the long term.

The second consideration for establishing the risk levels was the smaller attack surface of the database and the operating system (there are fewer administrators than there are users); in addition, the controls over the segregation of duties that are in place for individual financial primes (Operating System (OS) administrators versus Database (DB) administrators) mitigates risks in the DB and OS realms even further.

## 2.1 Improve Sustainability of Monitoring Controls

Wherever possible, a control should flow naturally from the work that is being controlled. When that is not is possible, controls should be optimized to support the business process. In this way, work done to carry out the control also contributes to the business being conducted, thus reducing the incremental costs imposed by the control. When a control is added on to a business process with little integration or optimization, it simply becomes something else that needs to be done with scarce time and resources.

A number of the monitoring tools that were developed to address the control weaknesses identified in the Phase 2 Audit Readiness Assessment report were found not to have been optimized to help the business units perform the monitoring function. For example, in order to be able to monitor changes to Merlin accounts (adding an account, changing the responsibilities for an account, or deactivating an account), system managers take monthly snapshots of the active users in the system and store them in a .PDF file for future monitoring and auditing. Then, during monitoring, to determine which accounts have changed in the system during a given month, the monitor conducts a manual comparison of the two snapshots looking for differences.

From interviews, it appears that the business and IT areas focused their efforts on meeting the recommendations from the Phase 2 Audit Readiness Assessment. The controls that were implemented will remediate the deficiencies; however, in order for the monitoring to be sustainable over the long term, the automation of certain activities needs to be considered.

The audit team observed that remediation activities were put in place to address monitoring deficiencies using the existing level of resources. Through regular system upgrades and the introduction of new, more robust technologies, IT financial monitoring controls will undergo further improvements and the requirement for manual interventions should diminish. This is a continuous improvement process that is encouraged and that will, over time, maximize new and improved technologies.

The Chief Financial Officer (CFO), in consultation with the Chief Information Officer (CIO), should review the original findings presented in the Phase 2 Audit Readiness Assessment report and the control remediations implemented with an aim of enabling a better automation of the monitoring that is required to address the control weaknesses. Based on an understanding of the business value of the monitoring being recommended, the design of the tools and processes that have been developed should be reviewed to see how they could be modified for better integration into the business process and enhanced value to the business units, given the Department's current reality in terms of risk tolerance and resource availability.

**Recommendation**

The CFO should develop a plan for re-engineering the monitoring controls over the financial systems within a continuous improvement strategy in order to integrate them into existing business processes, reduce costs and improve sustainability.

**Management Response**

*Agree. IES is currently developing the Departmental Financial Management System (DFMS) plan, which will ensure continuous system monitoring and address central agency requirements on standard business processes and ensure proper integration.*

## 2.2 Work Plan Required for Outstanding Items

The audit team faced two difficulties regarding a number of the controls it assessed. In some instances, the team was  unable to do the level of testing required to provide a higher level of assurance. In other cases, it found issues with control designs that may or may not constitute an ongoing risk to the Department’s objectives over time.

Many of the controls that were reviewed were only implemented on April 1 of 2011, almost at the end of the audit fieldwork. Consequently there was insufficient time for transactional evidence of account controls to accumulate to allow effectiveness testing to proceed.

To be able to produce auditable financial statements, the CFO will have to reconsider the management action plan provided in response to the Phase 2 Audit Readiness Assessment report. Given the recent implementation of the controls in 2011, a number of items are complete or well advanced, but further work is required to address them fully.

The audit results for the 25 recommendations for improving IT financial controls are presented in Annex 1 to this report and are summarized as follows:

- Eleven controls were found to have been well addressed by the work to date. However, additional work is required to complete the documentation and to integrate these controls into standard work routines.
- Two controls were found to have been met, but moderate issues with them remain. Both controls pose a medium level of residual risk to the Department.
- Twelve controls were found to be largely effective. Only minor issues remain. These controls pose a low level of risk to the Department.

The audit team observed that residual work remains for the 12 low-risk controls and the 2 medium-risk controls. The work would use the results of the audit and the audit team’s own testing to refresh of the original work plan that responded to the Phase 2 Audit Readiness Assessment. Alternately, the team could develop a new work plan to address the outstanding issues. Either approach would make the remaining work more effective, easier to integrate into standard work routines, and more focused on completing the items using a risk-managed approach.

**Recommendation**

The CFO should develop a work plan to address the completion of activities outstanding from the work plan arising from the Phase 2 Audit Readiness Assessment report.

**Management Response**

*Agree. A work plan that addresses all outstanding items from the Phase 2 Audit Readiness Assessment Report 2009 Audit has been prepared.*

## 2.3 A Program of Continuous Monitoring should be Implemented

To be effective, monitoring activity must be carried out in a consistent manner and must be well documented. In particular, documentation should make it clear why the monitoring is taking place, what distinguishes acceptable performance from unacceptable performance, when the monitoring happened, who carried out the monitoring, what was found and what, if anything, was done as a result of the activity. Finally, we expect to see the results of the monitoring activity reported back to management so that the managers can make decisions about improvements to policy, procedures and controls.

The recommendations arising from the Phase 2 Audit Readiness Assessment require that many controls be subject to periodic review (monitoring). The audit team found that processes surrounding this monitoring are documented and managed as individual activities, and that the monitoring controls are independently designed and operated without reference to what they are meant to accomplish—namely, to provide assurance that the IT financial controls are operating as required in order to make the financial statements auditable.

It appears that, due to the large number of findings that arose from the Phase 2 Audit Readiness Assessment, management decided to tackle the recommendations one at a time rather than trying to come up with a plan for addressing them together.

Dealing with monitoring controls on a case-by-case basis means that the monitoring may not be carried out consistently across controls or by different individuals. Not having an overall strategy for carrying out the monitoring activity may also lead to inefficiencies and may make it more difficult to share lessons learned from one activity to another.

Monitoring of IT financial controls should be considered as a single activity. The monitoring activity should be managed under one umbrella function. The purpose of the monitoring activities should be clearly articulated along with indicators of what constitutes good and bad practice. The monitoring should directly support the financial and IT governance processes and should give management the information it needs to establish that controls are working as planned, and to make decisions about changes in the control environment that are reasonable, given the risk appetite and the availability of resources. Logs of monitoring activity should be maintained as well as evidence necessary for audit follow-up activity. Finally, key indicators should be developed to describe the effectiveness of the IT financial control environment to management.

After completion of the work plan (refreshed or new—per section 2.2 above), a program of continuous monitoring should be implemented by the Finance and Corporate Services

Branch (FCB) to track the effectiveness and sustainability of the monitoring controls. The results of this continuous monitoring would assist in quality assurance and the continuous refinement of the monitoring functions so that they remain in an optimal state of maturity for the risk tolerance environment.

**Recommendation**
The CFO should develop a strategy for the continuous monitoring of IT financial controls, which should be part of an overall strategy of monitoring internal controls.

**Management Response**
*Agree. The strategy for the continuous monitoring of IT financial controls will be incorporated into the EC DFMS for 2011–2012. In addition, Environment Canada is looking to invest in non-proprietary software to facilitate continuous monitoring of financial controls.*

## 2.4 Identity and Access Management Controls Do Not Leverage Information Available in Human Resource (HR) Systems

There should only be one system of record for any given piece of information. Wherever practical, systems should leverage existing information from systems of record rather than trying to maintain a separate copy of that information.

The audit team found that many of the controls related to identity and access management, especially those that are detective in nature (such as those involving monitoring), would be more effective if they could leverage information already available in the HR systems (such as, for a given period, lists of employees who had left the Department, lists of employees who had joined the Department and lists employees who had changed their roles).

To accomplish this efficiently, the financial systems would have to include a unique identifier on their user records that is shared with the HR system.

Historically, designers have often ignored the availability of information in HR systems because of the difficulties dealing with associated privacy concerns.

Lack of access to this pre-existing information means that there is no independent source of information with which to validate account management activities that have taken place. This is particularly true for detective controls such as those used for monitoring account management activity after the fact.

Further, it means that data is stored redundantly and must be maintained twice, with the attendant risk of a loss of integrity. The design of the monitoring controls will be less effective without a unique, single source of good-quality information. Without such a single source, monitors who check what account-based activity took place will then have to find substantiating documentation of who authorized the activity. If HR data were available, it would be independent and would improve the segregation of duties and allow for a more automated validation of account activities.

IT financial controls related to identity and access management should leverage information already available in various HR systems. Enabling this activity may require a short-term allocation of resources by the Department and engagement on the part of the Assistant Deputy Minister for HR, the CIO and the CFO.

In particular, the design of detective controls like those used in monitoring account management activities should be optimized to make use of HR information (such as employees who have left the Department in a given period, or employees who have joined the Department and employees who have changed roles or positions).

Further, the account management tables in the financial systems should be modified to include a unique identifier for account holders that are shared with HR and contractors' management systems.

**Recommendation**
The CFO and the Assistant Deputy Minister for HR should establish a strategic plan for leveraging existing user identification for use in the financial systems.

**Management Response**
*Agree. Access to corporate key interfaces will be finalized for enhanced controls over user identification in the system.*

# 3 CONCLUSION

Since the release of the Phase 2 Audit Readiness Assessment report in March 2009, significant effort has been made to address the recommendations and underlying findings regarding the 25 issues of IT financial controls. The financial system has undergone major upgrades in its platform and functionality. In particular, in the past 8 months, the Department has migrated the system from a UNIX platform to a LINUX platform, added the asset life-cycle management functionality and patched a number of security threats.

For the work plan arising from the Phase 2 Audit Readiness Assessment of March 2009 and which had a completion date of March 2011, we conclude that substantial progress has been made in addressing the 25 IT financial control recommendations. All high-risk areas of control weakness have been mitigated but further work is required to address them fully. Eleven controls were found to be well addressed by the work undertaken to date. Twelve of the remaining controls were found to be largely effective, with only minor issues that still need to be addressed—each control posing a low level of risk to the Department. The final two controls were found to still have moderate issues to address, each control posing a medium level of residual risk to the Department. The first of these two controls involves ensuring that no active accounts assigned to former employees remain active; and the second, ensuring that activity by privileged Merlin users is monitored.

When the audit fieldwork began in earnest in December of 2010, the review team found that almost none of the policy and procedural work had been accomplished. However, by the time the audit team was able to begin testing, this situation had been largely reversed, with almost all of the policy and procedural work having been completed. This was accomplished in an environment when the resources of the Finance and Corporate Services Branch were involved in the implementation of the major change in platforms in November of 2010, as well as the work involved for the financial year-end.

# Annex 1
# Audit Criteria

1. Remedial actions in response to the recommendations of the Phase 2 Audit Readiness Assessment have been undertaken and have been effective in addressing the findings from that report.

## Sub-criteria

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 1 | User accounts for contractors and temporary staff can be identified | Low risk | Yes | Yes | Yes | While the January review indicated that little work had been done surrounding the policy and procedures for this control, a thorough document review and interviews during the testing phase indicated that, as of April 1, 2011, the basic tools available to make this control work have been in place, including fields for establishing employee types and for end-dating accounts for term, contract and casual employees.<br>The implementation of the control was announced Department-wide in late March of 2011. During interviews, we were told that, [Text removed to protect the security of the system]<br>As the control was only put in place on April 1, 2011, [Text removed to protect the security of the system] there was insufficient new user activity to test, and as a result the audit team could not conclude on how well these controls are working. The auditors did find a number of [Text removed to protect the security of the system] The audit team has recommended further audit follow-up work after the September 30 date to establish the effectiveness of the control as implemented.<br>Given that appropriate procedures and policy for the new controls |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| | | | | | | appear to be in place and [Text removed to protect the security of the system], we feel it poses a low risk to the Department's ability to provide auditable financial statements. |
| 2 | Controls related to identity management in PWGSC service provisions have been specified in the service level agreement SLA | Met | No | Yes | No | As per a review of the current SLA with PWGSC (February 2011), Environment Canada now has the necessary read-only activity for performing monitoring and audit activity. |
| 3 | Ongoing segregation of duties has been assured | Low risk | Yes | Yes | Yes | Policy and procedural documentation are appropriate and supporting IT-based tools are available, but insufficient evidence of monitoring was available for testing, leaving the audit team unable to conclude on the operating effectiveness of the control. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 4 | Generic user accounts are identified and their activity is monitored | Met | Yes | Yes | No | The audit team found evidence that generic accounts were reviewed in March 2011, but there was no evidence of an ongoing periodic review of these accounts. There was evidence of follow-up action resulting from the March review, deactivating all but 11 accounts. Two of these 11 remaining generic accounts are required by Oracle to perform functions. Interviews with the responsible business managers revealed that they were aware that there are 9 remaining generic accounts; that the accounts are being used for an ongoing initiative; and that their use is being actively monitored.<br>The original finding did not require that there be no generic accounts. It only required that the business managers know the purpose of the accounts, determine who was monitoring the accounts and document people who had access to an account's password. Based on this understanding and the availability of compensating controls, we believe that this criterion has been met.<br>Activity related to accounts of this type should continue to be monitored closely.<br>The audit team responsible for testing the control found that this control was met with only minor issues. However, when we reviewed the original finding and recommendation, we found that this sub-criteria had been met. We do recommend that, when generic accounts are used, their purpose and use be well documented and activity carried out by the accounts be monitored closely. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 5 | No active accounts are assigned to former employees | Medium risk | Yes | No | Yes | Evidence was provided showing that a custom report has been created listing active users with last login date. A Last logon date of active users report, generated 30 March 2011, was also provided. [Text removed to protect the security of the system] Follow-up audit should be planned to confirm that these accounts are still required.<br>Policy and procedure documentation does not indicate the frequency of review of the Last logon date of active users report or the individual responsible for reviewing, analyzing and storing this report. Through inquiry it was confirmed that the Last logon date of active users report will be generated and stored for audit purposes on a go-forward basis.<br>A copy of the new draft Employee Separation Clearance Report and the new draft directive on employee separation clearance were provided. It was confirmed by inquiry that the Employee Separation Clearance Report must be signed off by Informatics and Finance to ensure that proper access to Merlin is deactivated.<br>Given that the control was only put in place in April 2011, evidence was insufficient to provide assurance that this control is effective.<br>[Text removed to protect the security of the system]<br>Given the compensating controls, we feel that the residual risk that arises due to our inability to test this control is medium. Policy and procedure documents could be enhanced in the area of reporting departures of account holders, including a description of the nature and timing of monitoring. [Text removed to protect the security of the system] |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 6 | Merlin application user accounts are reviewed periodically | Low risk | Yes | Yes | Yes | Based on the newly implemented procedures, Environment Canada should have a good understanding of which Merlin application accounts are active, what responsibilities those accounts should be associated with, and the status of employment of the account holders. Once this baseline information is available, we consider that the described ongoing monitoring strategy will address the original March 2009 findings and associated recommendation.<br>While at the present time there is insufficient evidence to conclude that the process is operating effectively, we find that the policy and procedure environment and the associated IT controls provide sufficient compensatory control to result in a low level of residual risk. Audit follow-up work should be considered for the periods after September 2011 to establish how effective the monitoring process is. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 7 | User authentication is monitored at the OS, database and application levels to identify suspicious activity | Met | Yes | Yes | Yes | During document review, the audit team saw evidence that reports are available to monitor unsuccessful logins at both the application and the database levels. [Text removed to protect the security of the system]<br>Through interviews the audit team was informed that monthly reviews had not been performed in the past but that one was carried out on March 31, 2011. During interviews the audit team was informed that the plan is to perform [Text removed to protect the security of the system] reviews of unsuccessful logins at both the database and the application levels on a go-forward basis. [Text removed to protect the security of the system]<br>Policy and procedural documentation for application and database failed login monitoring is appropriate. While monitoring of failed login attempts has been found to be adequate, the monitoring should be documented in terms of what it is meant to accomplish, when it is conducted, by whom, what was found and what if any actions arose from the monitoring process. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 8 | Activity by privileged Merlin users is monitored | Medium risk | Yes | No | Yes | There are two methods of monitoring activity within Merlin.<br>The first method is governed by the Signon Audit Level, which monitors activity of users at one of four levels. The most detailed level is the form level. At this level, user activity is stored when the user logs in, opens or closes a form, or prints something.<br>The second method for monitoring activity is governed by the Audit Trail system profile option. This method of auditing records database changes at the record level, storing a before-and-after image for every change made. This method of creating an audit trail is very powerful, but it also consumes huge amounts of resources. It is set for a table or a group of tables.<br>[Text removed to protect the security of the system] |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 9 | User access control functions are monitored at the application level | Low risk | Yes | No | Yes | For this control to work, administrators need to know when someone has left the Department. The administrators then need to react by deactivating the associated Merlin account in a timely fashion. Administrators now have three ways of finding out when a user has left the Department.<br>First, they will soon have the revised Employee Separation Clearance procedure and directive. The revised procedure specifies more clearly the requirement to notify Finance and CIOB that an employee has left. The new procedure also requires the Branch to disable the employee's access to the corporate IT infrastructure and financial systems.<br>Second, administrators are maintaining a monthly snapshot of active users on the system. By comparing one month to the next, it will be possible to see which users have been added to the system, been deactivated on the system or had a change in access privileges during the month. This control will not help system mangers deactivate accounts, but it does provide a tool for monitoring how well the other parts of the control are working.<br>A third method provided by a new report is available that shows the last login date for each employee, and employees that have not logged in recently can be subjected to further scrutiny.<br>Taken together, these three strategies mitigate the likelihood that an account will remain active for a departed employee.<br>Finally, since access to Merlin is only available across the LAN if the user's active directory account has been disabled, the presence of an active Merlin user account is less of a risk ([Text removed to protect the security of the system]). |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| | | | | | | We have noted, however, that the tools for accomplishing this work are not optimized for use by the business area. This weakness may lead to a control that is unsustainable over time because it will take too many resources to perform. [Text removed to protect the security of the system]<br>Policy documentation can be enhanced for monitoring and reporting related to the [Text removed to protect the security of the system]. Insufficient evidence was available for testing this control and as a result we were unable to conclude on its operating effectiveness with an audit level of assurance. We do find, however, that the anticipated control to be provided by the new directive and forms [Text removed to protect the security of the system] will mitigate this risk to a low level by reducing the likelihood [Text removed to protect the security of the system] The detective controls that are now available (monitoring the active user reports) will further mitigate this risk. Even so, we still find that these monitoring controls have not been optimized for this task, increasing the risk that monitoring will be unsustainable over time. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 10 | Merlin application password controls are monitored | Met | Yes | Yes | No | On April 1, 2011, a new password control regime was implemented at Environment Canada. The audit team found that the new regime is an effective control of passwords for Merlin users and that it addresses all of the concerns raised in the March 2009 report finding and fulfills all of the recommendations from that report.<br>The audit team reviewed the password settings in the application configuration and found that the settings meet or exceed the settings recommended in the Phase 2 Audit Readiness Assessment.<br>Further, when the controls were tested in the presence of the audit team, they were found to work as established. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 11 | User activity is logged at the application level to the form level | Met | Yes | No | No | We found through interviews and document review that the recommended level of access logging has been set in the system. We find that this sub-criterion has been met and that the control is adequately implemented. |
| 12 | Database administrator's accountability is assured [Text removed to protect the security of the system] | Low risk | Yes | Yes | Yes | By reviewing the roles assigned to the database administrator's individual accounts[Text removed to protect the security of the system]<br>As was noted in the Phase 2 Audit Readiness Assessment report, this can pose a significant risk to the organization: [Text removed to protect the security of the system]<br>The audit team also noted that [Text removed to protect the security of the system] |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| | | | | | | We were told that the DBA team with access to Oracle Financials is relatively small, they work in close proximity, and the individual DBAs are cleared to the secret level. Finally, with the [Text removed to protect the security of the system]  These compensating controls mitigate somewhat the risks posed by the [Text removed to protect the security of the system].<br>We find that this control is ineffective, but that the compensating controls noted above do reduce the level of risk associated with the weakness to low. |
| 13 | System database accounts are identified and have appropriate password controls | Low risk | Yes | No | Yes | The tools are now in place to make this control work, but there was insufficient evidence to conclude that the tools are being used to effectively mitigate the risks described in the Phase 2 report. [Text removed to protect the security of the system]<br>Further, the tools that have been proposed for this activity are not optimized to help system managers monitor this activity. This may make the monitoring process unsustainable over time.<br>Policy and procedural documentation does not indicate that passwords will be changed on a regular basis and insufficient evidence was available to test the control's effectiveness. As a result, the audit team was unable to conclude on the operating effectiveness of controls.<br>Given the weaknesses in the documentation [Text removed to protect the security of the system]  which is contrary to best practices, we find that this control is still ineffective but poses only a low level of risk to the Department's ability to produce auditable financial statements. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 14 | Merlin database user accounts are periodically reviewed | Met | Yes | No | No | The audit team found through document review and interviews that this control is effective. We found that the tools are in place to allow for monitoring the creation/change/deactivation of Merlin database accounts. However, as with other monitoring controls in this system, we find that the tools that have been developed are not optimized for the job for which they are intended. This means that the monitoring controls may not be sustainable over time. |
| 15 | Standard procedures have been established for creating new database accounts | Low risk | Yes | Yes | Yes | The audit team found insufficient evidence to conclude that standard procedures or controls exist relating to requesting, approving, creating and segregating duties for new database accounts and access rights. We further found that the control that is in place is ineffective in that documentation made it appear that users could request enhanced access to the production platform under their own authority. Even though this turned out not to be the case, the lack of standards on how to record this type of activity leaves the Department at a low level of risk. |
| 16 | Standard procedures have been established to ensure that database account privileges are changed when users change positions or responsibilities | Low risk | Yes | Yes | Yes | The audit team found insufficient evidence to conclude that standard procedures or controls exist relating to requesting, approving, creating and segregating duties for new database accounts and access rights. We further found that the control that is in place is ineffective in that documentation made it appear that users could request enhanced access to the production platform under their own authority. Even though this turned out not to be the case, the lack of standards on how to record this type of activity leaves the Department at a low level of risk. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 17 | Standard procedures have been established for [Text removed to protect the security of the system] | Low risk | Yes | Yes | Yes | Policy and procedural documents do not indicate that monitoring will be conducted on a regular basis. [Text removed to protect the security of the system]<br>Given that the tools for monitoring this type of activity were only implemented in April of this year, there has been insufficient time to accumulate records to test. Given the inability to test this control and the weakness in the documentation, the audit team found this control to be ineffective. [Text removed to protect the security of the system]. However, given compensating controls like the plan to monitor this activity in the future, we feel that the level of risk posed by the control weakness is low. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 18 | Standard procedures have been established to ensure that program changes go through testing and quality assurance prior to being promoted to production | Low risk | Yes | Yes | Yes | Through document review it was found that the documentation for this process is out of date, still making reference to the Software Management Board, which was recently replaced by the Change Control Board (CCB).<br>Other documentation indicates that the CCB formally approves, rejects or defers change requests. The CCB is supposed to meet on a monthly basis. Per inquiry it was confirmed that the CCB is a new board that has not yet had a formal meeting. The meetings are to occur on a go-forward basis.<br>Through inquiry it was confirmed that a form is used to capture approval by all module leads before the ticket or change request is promoted to another environment. A signed copy of the form is kept by the manager and test script results are kept in a binder by the module lead. A sample form was provided.<br>The audit team had asked for a system-generated list of program changes so that that list could be used as a sample frame from which to select a sample for testing. As the list could not be generated, testing was not possible. In absence of the ability to produce such a list, some mechanism is required for generating a log of program changes by date that indicates who approved each promotion of code from one platform to another. Follow-up audit work should consider using the output from the ticketing system as a sample frame.<br>There is an opportunity for improving the documentation of program change procedures and the program changes themselves. While insufficient evidence was provided to allow us to conclude on the risk at an audit level of assurance, we find that this criteria was largely met with minor issues and that these issues pose a low level of risk to the Department’s objectives. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 19 | The test environment is identical to the production environment | Met | No | Yes | No | It is not possible to have a completely identical test environment unless the test environment is maintained on an identical but physically separated network. The test environment must exist in a different Oracle instance which, by necessity, has a different identifier if it is installed in the same network environment. There are a number of other installation parameters that must be different between the two environments so that the programs from one environment do not affect the databases on the other environment.<br>The audit team responsible for testing the control found it to be ineffective, but given the need to have some differences between the environments, the documented method of cloning and refreshing the production environment for use in test, development and QA is more than adequate and provides reasonable assurance that code in one environment will act the same way as the same code in the other environment.<br>Policy and procedural documentation is acceptable and, based upon the method used for cloning the production environments, we find that this sub-criterion has been met. |
| 20 | Change request forms for Merlin database and application are appropriately authorized | Met | Yes | Yes | No | Confirmed through observation and inquiry that the change request template enforces a digital signature. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 21 | Formal processes exist for monitoring changes made to the Oracle database and to the Merlin application | Met | Yes | Yes | No | It was confirmed through observation and inquiry that the QA team will sign off on the release of change request tickets. |
| 22 | Post implementation review work by the QA team is documented and retained | Met | Yes | Yes | No | It was confirmed through observation and inquiry that the QA team will perform post-implementation review and retain evidence related to the review. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 23 | Operating system user access is monitored | Low risk | Yes | No | Yes | The audit team responsible for the testing did not find sufficient documentation describing how operating system accounts are managed. Further, the audit team noted a few anomalies like evidence of a problem during the upgrade of the system from the UNIX platform to its current LINUX platform. It is possible that these problems would have been caught before they occurred if adequate standards had existed. The audit team found a few isolated cases that need follow-up via the monitoring process and in future audits.<br>We discovered by inquiry that Environment Canada employees only ever get Read/Execute access to file shares on the OS. They are never granted admin rights on the OS.<br>While insufficient information was available for comprehensive testing, the audit team has concluded that this control and accompanying documentation are inadequate. Given that the level of access granted to Environment Canada employees is restricted to file access in specified shared areas, the level of risk posed by this weakness is low. [Text removed to protect the security of the system]  will be required to ensure that this risk remains low. |
| 24 | A list of people authorized to request that PWGSC create OS accounts is created and maintained | Met | Yes | Yes | No | Through inquiry and document review we have discovered that PWGSC has been provided with a list of Environment Canada staff who can authorize the creation, modification and/or removal of operating system accounts for Environment Canada employees. Further, through inquiry we have determined that a separate list exists at PWGSC that identifies which Environment Canada employees must be notified when an operating system account is added, changed or deactivated. We have concluded that these two controls, taken together, provide adequate control. |

| Sub-criteria No. | Description | Overall Conclusion | Continuous Monitoring Required? | Control Design sustainable? | Additional Audit Work Required? | Comments |
|---|---|---|---|---|---|---|
| 25 | Processes exists to ensure that user accounts for departing employees are deactivated in a timely fashion | Low risk | Yes | Yes | Yes | The audit team responsible for testing this control found insufficient evidence to provide an audit level of assurance that this control is adequate. Coupled with a lack of current documentation surrounding the process, the audit team concluded that the control was ineffective.<br>Through document review and inquiry, we did discover that the anticipated directive (and supporting forms and procedures) on employee separation clearance is expected to provide IT staff with advance information about the departure of an employee. Part of the associated IT process is to ensure that all system accounts are deactivated for employees as they depart. This new directive is expected to take effect in July of 2011. Further, the new service level agreement with PWGSC gives Environment Canada managers read-only access to the operating system, enabling future monitoring and auditing of the process.<br>With these two improvements to the control environment expected in the near future, we conclude that this control weakness only poses a low level of risk to the Department. To maintain this low level of risk, follow-up audit work must be carried out to ensure that monitoring is taking place and that the new directive and associated procedures are approved and implemented. |