Section 8

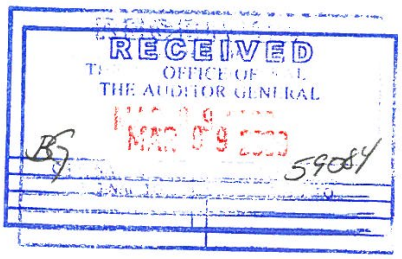
Update on the implementation of recommendations from:

Managing Government's Payment Processing

May 2008

April 2009

BRITISH COLUMBIA
The Best Place on Earth



184168

February 27, 2009

Bill Gilhooly
Assistant Auditor General
Office of the Auditor General
PO Box 9036 Stn Prov Govt
Victoria BC V8W 9A2

Dear Bill Gilhooly:

Re: Follow-up review of your report on *Managing Government's Payment Processing – May 2008*

As requested, please find attached our updated self-assessment regarding actions taken in response to the recommendations in your audit report named above. I understand that this response, including the Recommendation Status Summary and the Progress in Implementing Recommendations Form, will be printed, unedited, in your semi-annual follow-up report, to be released April 1, 2009.

We were pleased and reassured by the auditors' conclusion in the report that "adequate controls are in place to manage risks associated with government's payment processing". We are further strengthening controls around payment processing in government by addressing the recommendations in the report. These actions include further enhancements in the areas of management monitoring and review, access, segregation of duties and documentation. To date, all recommendations have been addressed in some way, with 30 of the 34 recommendations either fully or substantially implemented or addressed through an alternate action.

.../2

Ministry of Finance | Office of the Deputy Minister | Mailing Address: PO Box 9417 Stn Prov Govt Victoria BC V8W 9V1 www.gov.bc.ca/fin | Location Address: Room 109 617 Government Street Victoria BC

The attached documents are a combined response from the Ministry of Finance (Banking/Cash Management Branch, Provincial Treasury) and the Ministry of Labour and Citizens' Services (BC Mail Plus and Corporate Accounting Services, both branches within Common Business Services).

I trust that this is satisfactory.

Sincerely,

Chris Trumpy
Deputy Minister

Attachments

pc: Lori Wanamaker
Deputy Minister of Labour and Citizens' Services

Graham Whitmarsh
Associate Deputy Minister of Revenue

Jim Hopkins
Assistant Deputy Minister, Provincial Treasury
Ministry of Finance

Richard Poutney
Assistant Deputy Minister, Common Business Services
Ministry of Labour and Citizens' Services

Cheryl Wenezenki-Yolland
Comptroller General
Ministry of Finance

Vern Burkhart
Executive Director, Procurement and Supply Services
Ministry of Labour and Citizens' Services

Nashater Sanghera
Executive Director, Corporate Accounting Services
Ministry of Labour and Citizens' Services

RECOMMENDATION STATUS SUMMARY

Managing Government's Payment Processing

As at January 31, 2009

(*Please tick implementation status for each recommendation*)

Auditor General's Recommendations	Implementation Status				
	Fully	**Substantially**	**Partially**	**Alternative Action**	**No Action**
A. Administration and maintenance of access					
1. User and group access should be regularly reviewed to ensure that it is consistent with operational duties and responsibilities and that proper segregation of duties is maintained.	X				
2. Risks associated with the lack of segregation between those administering and monitoring security and those handling daily production activities, and between those maintaining daily system production and those developing and testing changes to production programs should be evaluated. Possible consequences and mitigations should be considered, including whether any residual risks are acceptable.				X	
3. Security profiles protecting payment, bank reconciliation and computer program files should include logging all change activities for later review.	X				
4. Procedures should be established and carried out to regularly monitor and investigate, as required, activities where changes are made to high-risk data and programs.		X			
5. Access to audit logs should be granted only on a "need to have" basis.	X				
6. The relationship and responsibilities between the Provincial Treasury Information Systems Branch and the Ministry of Finance Information Management Branch should be more clearly documented and communicated.		X			

Auditor General's Recommendations	Implementation Status				
	Fully	Substantially	Partially	Alternative Action	No Action
B. Generation of payment and bank reconciliation files and transfer to MVS for further processing					
Generation of payment files in the UNIX environment					
7. Management should review access to ensure proper segregation of duties between staff able to set up and run production processes and those responsible for development activities.				X	
8. Access to the payment file information should be further restricted to ensure its confidentiality and integrity.	X				
9. A review of "root" access relative to job descriptions and requirements should be performed, and management should formally approve "root" access in each case. Any excessive access should be removed.	X				
10. Management should investigate whether software could be used to delegate "root" user capabilities, and audit all activities with this authority.			X		
Use of File Transfer Protocol to transfer payment files to MVS					
11. Management should implement a more secure means of transferring files from UNIX to the mainframe environment. The method used should protect the confidentiality of logon credentials and data during transmission over the network.			X		
12. An audit trail of transaction counts and control totals should be implemented and checked on each file transmission. This would verify that information was not altered during the FTP process.				X	
Creation of EFT and cheque payment files and control files in the MVS environment					
13. To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files should be flagged,			X		

Auditor General's Recommendations	Implementation Status				
	Fully	Substantially	Partially	Alternative Action	No Action
so that when a change is made, the user is identified and logged for later review.					
C. Processing and release of EFT payments					
14. Banking and Cash Management should keep its EFT procedures manual current to ensure accurate guidance is provided to new employees and back-up staff.		X			
15. All instances of incompatible duties should be removed or additional monitoring activities added to manage the risk of accidental or intentional errors going undetected.		X			
16. Batch numbers should be traced to ensure all payment files are processed.	X				
17. There should be evidence to support control procedures have been performed. This would ensure that the initial payment information from ministries has been reconciled to the payment information received and processed by the bank.	X				
18. All program changes should be tracked and monitored to ensure they are approved and in compliance with change management policies.	X				
D. Processing and printing cheques					
19. Several monitoring controls, such as access logs and staff lists, should be improved.	X				
20. Policies and procedures for staff should be updated, including those pertaining to cheque stock movements, testing procedures, reconciliations, and security measures.	X				

Auditor General's Recommendations	Implementation Status				
	Fully	Substantially	Partially	Alternative Action	No Action
21. The cheque inventory tracking application should be password-protected and key cells locked to prevent accidental erasure and alteration.	X				
E. Management of the status of payments					
22. Policies and procedures for managing the status of payments should be regularly reviewed and updated for new and back-up staff.		X			
23. Banking and Cash Management staff should communicate to ministries the importance of complying with policies and procedures for cancelling and re-issuing cheques, as outlined in government's financial policy manual.		X			
24. All program and data changes should be tracked and monitored to ensure they are approved and complying with policy.	X				
25. The summary report of paid cheque data should be regularly reviewed to ensure that the data was successfully loaded into the system.	X				
26. Roles and responsibilities should be reviewed by management with the aim of minimizing incompatible duties with respect to processing undeliverable and unclaimed cheques.	X				
27. Review of daily returned items should be performed regularly. This should be done by staff not involved in processing or authorizing returned items.	X				

Auditor General's Recommendations	Implementation Status				
	Fully	Substantially	Partially	Alternative Action	No Action
28. There should be evidence supporting comparison of the automated funds transfer (AFT) recalls confirmation report with the email notifications received from ministries.	X				
29. Replacement cheque records should be regularly reviewed by management to ensure they are complete and no duplicate payments have occurred.				X	
F. Reconciliation of payments to the general ledger					
30. Specific reference should be made in the maintenance process manual to the change management processes needed for applications running in the MVS mainframe environment.	X				
31. To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files should be flagged so that when a change is made, the user is identified and logged for later review.	X				
G. Back-up of program and payment files					
No recommendations					
H. Business continuity planning					
32. Banking and Cash Management Branch should update its business continuity plan promptly after each disaster exercise.	X				
33. Corporate Accounting Services should conduct an alternate site exercise.	X				
34. Corporate Accounting Services, Banking and Cash Management, and BC Mail Plus should jointly develop and maintain business continuity plans that will satisfy the minimum processing and printing requirements to enable critical payments to continue in the event of a disaster.			X		

PROGRESS IN IMPLEMENTING RECOMMENDATIONS FROM

Managing Government's Payment Processing

As at January 31, 2009

General comments

All recommendations have been addressed, either fully or to some extent. Remaining activities are scheduled and will be completed with due regard for existing and emergent priorities.

Progress by recommendation

For each recommendation, provide your assessment of implementation status as per the legend at the bottom of the page, and information on actions taken and results to support the status reported. Also include a work plan schedule for any recommendations not yet implemented.

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
Recommendation 1: User and group access should be regularly reviewed to ensure that it is consistent with operational duties and responsibilities and that proper segregation of duties is maintained.		
F	Auditing has been turned on to record all activities of user ids assigned to the Security Officer and Senior Technical Analyst. Resource Access Control Facility parameters have been set on all BankRec files allowing all activities of this group to be audited daily by the Corporate Accounting Services (CAS) Security Officer. Access for a number of user ids has been modified based on the report recommendations.	No further action required as this issue has been closed.
Recommendation 2: Risks associated with the lack of segregation between those administering and monitoring security and those handling daily production activities, and between those maintaining daily system production and those developing and testing changes to production programs should be evaluated. Possible consequences and mitigations should be considered, including whether any residual risks are acceptable.		
AA	In addition to management review, access restrictions, and a review of audit logs, CAS will be conducting a comprehensive risk evaluation on all aspects of security and will implement any necessary changes. CAS is also investigating alternative processes and procedures to address this and avoid budget impacts. These evaluations to be completed by March 31/09.	No further action required as this issue has been closed.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
	Auditing has been turned on, Resource Access Control Facility parameters have been set on all BankRec files and all activities will be audited daily by the CAS Security Officer.	
Recommendation 3: Security profiles protecting payment, bank reconciliation and computer program files should include logging all change activities for later review.		
F	Auditing has been altered to log changes, including user id, on all BankRec files. All activities are audited daily by CAS Enterprise Security Officer.	No further action required as this issue has been closed.
Recommendation 4: Procedures should be established and carried out to regularly monitor and investigate, as required, activities where changes are made to high-risk data and programs.		
S	A comprehensive Information Systems Branch (ISB) security review was completed June 2008. Accesses were reviewed and changes made accordingly. Audit logs are created and a project to create exception reporting was completed December 31, 2008.	Documentation of exception reporting review procedures to be completed by March 31, 2009.
Recommendation 5: Access to audit logs should be granted only on a "need to have" basis.		
F	All access to these datasets have been restricted to the production support group, Multiple Virtual Storage (MVS) scheduler support and system accounts.	No further action required as this issue has been closed.
Recommendation 6: The relationship and responsibilities between the Provincial Treasury Information Systems Branch and the Ministry of Finance Information Management Branch should be more clearly documented and communicated.		
S	Meetings were held between the ISB and the Information Management Branch to clarify security roles and responsibilities.	A formal delegation instrument is under development and will be in place by March 31, 2009.
Recommendation 7: Management should review access to ensure proper segregation of duties between staff able to set up and run production processes and those responsible for development activities.		
AA	CAS has outsourced the scheduling tool support function, however to mitigate risk CAS has one FTE staff member who also has the scheduling tool support duties and knowledge. This does fall within our	Corrective action plan initiated and currently underway. Target date for completion is March 31, 2009.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
	risk tolerance. Audit logging will be turned on within the scheduling product to monitor activities of support personnel. Each day's audit logs are monitored by the Enterprise Security Officer.	
Recommendation 8: Access to the payment file information should be further restricted to ensure its confidentiality and integrity.		
F	A new directory for the payment file was created and access has been restricted to only the resources delegated with responsibility for the nightly scheduling activities and support of the payment file transfer (currently 3). Access has been limited to only one user id.	No further action required as this issue has been closed.
Recommendation 9: A review of "root" access relative to job descriptions and requirements should be performed, and management should formally approve "root" access in each case. Any excessive access should be removed.		
F	A review of access was conducted and excessive access has been removed. Access by the Database Administrators (DBAs) has been removed and will only be granted for emergencies or limited cases during upgrade projects, on a temporary and controlled basis which are logged and monitored by the CAS Enterprise Security Officer. CAS has implemented an outsourced service provider model with respect to DBA resources. DBA access is formally approved for each resource by the Director of Technology Operations. "Root" access is owned and monitored by Workplace Technology Services (WTS) as part of the Shared Services Hosting Service. WTS Hosting resources with root access are approved by WTS Management. CAS contacted WTS to confirm that root access is reviewed regularly and that no inappropriate access was in place.	No further action required as this issue has been closed.
Recommendation 10: Management should investigate whether software could be used to delegate "root" user capabilities, and audit all activities with this authority.		
P	CAS is not aware of any software delegation tools that would prevent root access users from being able to edit the audit logs. "Root" access is owned and monitored by WTS as part of the Shared Services Hosting Service. WTS Hosting resources with root access are	Corrective action plan initiated and currently underway. Target date for completion is March 31, 2009.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
	approved by WTS Management. CAS communicated the Auditor General's recommendations to WTS.	
Recommendation 11: Management should implement a more secure means of transferring files from UNIX to the mainframe environment. The method used should protect the confidentiality of logon credentials and data during transmission over the network.		
P	CAS has implemented an alternate encryption software package to protect the confidentially of the transmission. CAS is reviewing the WTS File Transfer Protocol Secure (FTPS) package to determine feasibility of creating a more secure transfer connection. The review will be completed by March 31, 2009.	Corrective action plan initiated and currently underway. Target date for completion is March 31, 2009.
Recommendation 12: An audit trail of transaction counts and control totals should be implemented and checked on each file transmission. This would verify that information was not altered during the FTP process.		
AA	CAS has implemented an encryption software package to ensure the information is not altered during the transmission.	No further action required as this issue has been closed.
Recommendation 13: To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files should be flagged, so that when a change is made, the user is identified and logged for later review.		
P	Audit logging has been turned on within the scheduler product. Each day's audit logs are monitored by the Enterprise Security Officer. CAS is currently investigating ways to enhance monitoring of DBA access. CAS investigated a configuration control software package, unfortunately, although this software is owned by WTS they have not made the service available to the ministries. Implementing a database specific product which can encrypt the data files, will require procurement and testing cycles. A project to implement DB Vault will begin by March 31st, 2009. CAS is not aware of any software delegation tools that would prevent root access users from being able to edit the audit logs. "Root" access is owned and monitored by WTS as part of the Shared Services Hosting Service. WTS Hosting resources with root access are approved by WTS Management. CAS communicated the Auditor General's recommendations to WTS.	Corrective action plan initiated and currently underway. Target date for completion is March 31, 2009.
Recommendation 14: Banking and Cash Management should keep its EFT procedures manual current to ensure accurate guidance is provided to new		

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
employees and back-up staff.		
S	All EFT (electronic fund transfer) procedures have been updated and are available to staff on the branch shared network drive.	A technical writing resource will be identified to collate the procedures into manual form. Target completion is June 30, 2009.
Recommendation 15: All instances of incompatible duties should be removed or additional monitoring activities added to manage the risk of accidental or intentional errors going undetected.		
S	A comprehensive ISB security review was completed June 2008. Accesses were reviewed and changes made accordingly. Audit logs are created and a project to create exception reporting was completed December 31, 2008.	Documentation of exception reporting review procedures to be completed by March 31, 2009.
Recommendation 16: Batch numbers should be traced to ensure all payment files are processed.		
F	All batches are matched to the incoming file notifications as evidenced by tick marks, and both releaser and reviewer initials. A systems project to enhance batch control edits was completed January 26, 2009.	No further action required as this issue has been closed.
Recommendation 17: There should be evidence to support control procedures have been performed. This would ensure that the initial payment information from ministries has been reconciled to the payment information received and processed by the bank.		
F	All payment files are matched to both the incoming file notifications from ministry feeder systems and file processing confirmations from our bank, as evidenced by tick marks, and both releaser and reviewer initials.	No further action required as this issue has been closed.
Recommendation 18: All program changes should be tracked and monitored to ensure they are approved and in compliance with change management policies.		
F	ISB has promoted greater staff awareness of the change management policy, and a ticket tracking tool is being used.	No further action required as this issue has been closed.
Recommendation 19: Several monitoring controls, such as access logs and staff lists, should be improved.		
F	All access for print operators and system analysts has been reviewed and updated as necessary. Off-hour access reports are routinely reviewed and authorized staff lists are maintained.	No further action required as this issue has been closed.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
Recommendation 20: Policies and procedures for staff should be updated, including those pertaining to cheque stock movements, testing procedures, reconciliations, and security measures.		
F	A cheque printing and distribution procedures manual has been developed documenting the process for MICR (Magnetic Ink Character Recognition) testing and the printing, control, sorting, distribution and reconciliation of cheques. The security manual is continually updated to reflect enhancements to security measures.	No further action required as this issue has been closed.
Recommendation 21: The cheque inventory tracking application should be password-protected and key cells locked to prevent accidental erasure and alteration.		
F	The cheque inventory tracking application has been password-protected with key cells locked.	No further action required as this issue has been closed.
Recommendation 22: Policies and procedures for managing the status of payments should be regularly reviewed and updated for new and back-up staff.		
S	All cheque management procedures have been updated and are available to staff on the branch shared network drive.	A technical writing resource will be identified to collate the procedures into manual form. Target completion is June 30, 2009.
Recommendation 23: Banking and Cash Management staff should communicate to ministries the importance of complying with policies and procedures for cancelling and re-issuing cheques, as outlined in government's financial policy manual.		
S	Advice is provided to clients daily and information bulletins are distributed to ministry contacts as required. Working in conjunction with the Office of the Comptroller General (OCG), draft changes to core policy have been presented to the Financial Officers Advisory Committee (FOAC) and feedback from the committee will be incorporated into the policy.	Client education is an on-going activity for the branch.
Recommendation 24: All program and data changes should be tracked and monitored to ensure they are approved and complying with policy.		
F	ISB has promoted greater staff awareness of the change management policy, and a ticket tracking tool is being used.	No further action required as this issue has been closed.
Recommendation 25: The summary report of paid cheque data should be regularly reviewed to ensure that the data was successfully loaded into the		

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
system.		
F	Review is evidenced by initials of the reviewer.	No further action required as this issue has been closed.
Recommendation 26: Roles and responsibilities should be reviewed by management with the aim of minimizing incompatible duties with respect to processing undeliverable and unclaimed cheques.		
F	Roles and responsibilities have been reviewed. Incompatible duties have minimized and any residual risk has been deemed acceptable.	No further action required as this issue has been closed.
Recommendation 27: Review of daily returned items should be performed regularly. This should be done by staff not involved in processing or authorizing returned items.		
F	The review is done daily and is evidenced by tick marks and initials of the reviewer. The reviewer is not the same staff member that processed the items.	No further action required as this issue has been closed.
Recommendation 28: There should be evidence supporting comparison of the automated funds transfer (AFT) recalls confirmation report with the email notifications received from ministries.		
F	Review is evidenced by tick marks and initials of the reviewer.	No further action required as this issue has been closed.
Recommendation 29: Replacement cheque records should be regularly reviewed by management to ensure they are complete and no duplicate payments have occurred.		
AA	Working in conjunction with OCG, draft changes to core policy have been presented to the FOAC and feedback from the committee will be incorporated into the policy. The proposed policy change identifies the issuing ministry as responsible for reviewing replacement cheque records and ensuring that no duplicate payments have occurred.	The final approved policy is targeted to be in place early in the 2009/2010 fiscal year.
Recommendation 30: Specific reference should be made in the maintenance process manual to the change management processes needed for applications running in the MVS mainframe environment.		
F	Maintenance process/procedural manuals have been reviewed and updated as recommended.	No further action required as this issue has been closed.
Recommendation 31: To provide assurance on the completeness of the manual change log, high-level profiles protecting computer program files		

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation

Self-Assessed Status	Actions Taken Since Report Issued	Results of Actions and/or Actions Planned (with information on implementation)
should be flagged so that when a change is made, the user is identified and logged for later review.		
F	Auditing has been altered to log changes, including user id, on all BankRec files. All activities are audited by CAS Enterprise Security Officer.	No further action required as this issue has been closed.
Recommendation 32: Banking and Cash Management Branch should update its business continuity plan promptly after each disaster exercise.		
F	The Business Continuity Plan (BCP) plan is updated regularly. A share-point site has been created for BCP documentation and a Business Continuity Officer has been hired to ensure documentation is maintained.	No further action required as this issue has been closed.
Recommendation 33: Corporate Accounting Services should conduct an alternate site exercise.		
F	During the Dec 4, 2008 MVS Hot Site and Data Recovery Plan (DRP) Technical Exercise, CAS staff performed their recovery tasks from the current alternate site.	No further action required as this issue has been closed.
Recommendation 34: Corporate Accounting Services, Banking and Cash Management, and BC Mail Plus should jointly develop and maintain business continuity plans that will satisfy the minimum processing and printing requirements to enable critical payments to continue in the event of a disaster.		
P	During the Dec 4, 2008 MVS Hot Site and DRP Technical Exercise CAS worked jointly with BC Mail Plus (BCMP) to confirm that processing and printing requirements are documented and exercised. CAS also confirmed that the processing and interfaces between CAS and the Banking and Cash Management branch (BCM) are functioning as expected. CAS will continue to work with BCMP and BCM to confirm continuity plans. Participants have been identified for a joint working group to identify and document the articulations between the existing CAS, BCM and BCMP Business Continuity Plans. Meetings will be scheduled prior to March 31, 2009.	DRP Testing was completed however it was inconclusive since the CAS generated Electronic Funds Transfer data was not used to ensure that electronic fund transfers would occur as expected.

Status

F or **S** – Recommendation has been fully or substantially implemented
P – Recommendation has been partially implemented
AA – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding
NA – No substantial action has be taken to address this recommendation