Project No.: 062024

Review of Common Disbursement System

Ministry of Education

Internal Audit & Advisory Services
Office of the Comptroller General
Ministry of Finance
Province of British Columbia

Date of fieldwork completion: May 2009

Table of Contents

Section **Page No.**

Abbreviations

ALMD	Ministry of Advanced Education and Labour Market Development
CAB	Change Advisory Board
CAS	Corporate Accounting System
CDS	Common Disbursement System
DMU	Disbursement Management Unit
EFT	Electronic Fund Transfer
FAB	Funding and Analysis Branch, ALMD
FCB	Funding and Compliance Branch, MED
FASB	Financial & Administrative Service Branch, MED
IAAS	Internal Audit & Advisory Services
ID	Identifier
IDIR	Government Internal Directory
IT	Information Technology
ITMB	Information & Technology Management Branch, both ministries
K-12	Kindergarten through 12th Grade
MED	Ministry of Education
OCIO	Office of Chief Information Officer
WTS	Workplace Technology Services

Executive Summary

The Ministry of Education (MED) and Ministry of Advanced Education and Labour Market Development (ALMD) administer transfer payments to educational institutions, nearly $5 billon and $2 billion respectively in 2007/2008.

The Common Disbursement System (CDS) was implemented in 2005 to replace the previous Grant Payments System, to support the issuance and monitoring of the transfer payments to K-12 and post secondary institutions. Subsequently CDS has also been used for transfer payments to independent schools and public libraries. Internal Audit & Advisory Services (IAAS) was requested by Cabinet via the Ministry Specific Risk Review Process for 2008/09, to undertake a review of CDS to provide assurance on existing internal controls to the ministries. The purpose of the review was to assess the existence and effectiveness of the internal controls to ensure the integrity of the transfer payments processing in the CDS. Our fieldwork was conducted from March to May 2009.

Overall Conclusion

We concluded that the internal controls, over transfer payments processing in CDS, exist and are effective to ensure the integrity of the payments processes. We identified opportunities for the ministries to strengthen some of the internal controls over system security and to enhance business processes. In concluding on our objectives, the following observations and key recommendations have been made.

Application and System Environment Controls

CDS application security has logical security procedures to ensure only authorized staff have access to the financial functions and data, based on their role. Opportunities were identified to strengthen the ***[Information withheld to protect security of a system].***

The current Change Management Policy describes in detail the policies and procedures that Information & Technology Management Branch, both ministries (ITMB) should apply to manage and control changes to the computing environment. However this document does not describe the procedures to be followed in regard to emergency changes required for high priority changes. To enhance the current process, we have recommended that ITMB update the current policy to include procedures for emergency changes.

Application and Business Processes Controls

The CDS policy and procedures and other related procedures manuals are in place and adequate to guide ministry staff. Roles and responsibilities are clearly defined and communicated. Additional documentation on the roles and responsibilities of System Administrator is recommended to identify a clear segregation of duties over the production environment.

As CDS is a system used by MED and ALMD, the existence of the joint ministry Change Advisory Board is an important model for financial system governance to ensure the interests of the ministries are represented and to provide system management and advice on possible enhancements on CDS.

Internal controls over transfer payment processes are adequate and working as intended to ensure the integrity, authorization, completeness and audit trails of transactions. In addition, the attributes of reliability and availability of CDS output are generally achieved.

Additional observations and recommendations are described in the body of the report.

We wish to express our appreciation to the ministries' staff for their cooperation and assistance throughout this review.

Stuart Newton
Executive Director
Audit & Technical Services
Internal Audit & Advisory Service

September 2009

Background

In fiscal year 2007/08, the Ministry of Education (MED) administered approximately $5 billion in transfer payments to British Columbia's K-12 system, which serves over 590,000 public school students, 68,000 independent school students and 2,800 home-schooled children. The Ministry of Advanced Education and Labour Market Development (ALMD) administered nearly $2 billion in funding to 27 post-secondary institutions.

To facilitate better systems to support the issuance and monitoring of the transfer payments to K-12 and post secondary institutions, the ministries developed and implemented the Common Disbursement System (CDS) in spring 2005, replacing the previous Grant Payments System. CDS provides functionality to support business processes in setting up transfer payment activities, authorizing allocations, managing payments, handling budget changes, and monitoring expenditures.

The transfer payments currently issued within CDS and processed by Funding and Compliance Branch (FCB), MED, includes payments to:

- the 60 Public School Districts;
- the 258 Independent School Authorities; and
- the 240 public library facilities.

The payments through CDS to Post Secondary Institutions are processed by the Funding and Analysis Branch (FAB), ALMD.

Prior to its implementation in 2005, MED requested Internal Audit & Advisory Services (IAAS) to conduct a risk and control review of the CDS application system. The implementation in 2005 included only Public School District and Post Secondary Institutes' payments. IAAS provided one recommendation ***[Information withheld to protect security of a system]*** which was re-examined in this review.

IAAS was requested by Cabinet via the Ministry Specific Risk Review Process for 2008/09, to undertake a review of CDS to provide assurance on existing internal controls to the ministries. To undertake a review of CDS to provide assurance on existing internal controls to the ministries.

Purpose

The purpose of this review was to assess the existence and effectiveness of the internal controls to ensure the integrity of the transfer payments processing in CDS. The review considered the business risks and how the system controls assisted in addressing those risks.

Scope and Objectives

The scope and objectives of the review were as follows:

A. **Control Environment** (for the management of payments) – whether the control environment provides reasonable assurance on the reliability of the CDS management, operational, and security framework. We reviewed:

- ***policies and procedures*** – to ensure ministry management has established a policy framework and procedures related to transfer payments;
- ***roles and responsibilities*** – to ensure roles and authorities over the transfer payments process and system functions are clearly defined and communicated;
- ***application security design*** – to ensure logical security procedures are established to allow only authorized staff have access to CDS financial functions and data in accordance with their roles;
- ***segregation of duties*** – to ensure adequate segregation of duties are in place for the funding process and system functions;
- ***change management*** – to ensure formal change management procedures are in place to maintain the integrity of the data and application;
- ***continuous services*** – to ensure operating procedures and a backup process are in place, and are periodically tested and updated;
- ***compliance*** – to ensure a process exists to monitor compliance with related legislation in regard to timeliness of payments (*School Act* and *Independent School Act*); and

- ***management monitoring*** – to ensure appropriate management monitoring controls over the funding system are in place.

B. Business Processes and Application Controls – whether the designed controls within ***[Information withheld to protect security of a system]*** major functions of CDS ***[Information withheld to protect security of a system]*** provide reasonable assurance on the integrity and reliability of the application. Specific objectives within this component included:

- ***integrity*** – to determine whether controls over funding data entry and processing within CDS provide reasonable assurance that recorded transactions are valid, complete, accurate and timely;

- ***authorization*** – to establish whether designed controls provide reasonable assurance that recorded transfers are appropriately authorized in accordance with ministry and government policies and procedures;

- ***reliability and availability of CDS output*** – to determine whether information to be reported meets user requirement specifications and controls for reporting provide reasonable assurance that output is complete and accurate for management reporting;

- ***application integrity*** – to establish whether controls for data transfers within CDS and between CDS and Corporate Accounting System (CAS) provide reasonable assurance that interfaced data is complete, accurate, authorized and timely; and

- ***management trail*** – to determine whether critical transactions can be traced through the system and to the source/ originator.

The scope included only processes and systems managed within MED and ALMD (the ministries). We focused on transfer payment processes from the point where the calculation of transfer payment allocation is approved to the point where payment data is accepted into CAS for actual transfer or cheque payment. This review also included the reconciliation process between CDS and CAS.

Rather than reporting out by detailed objectives in the order listed above, we categorized our findings and recommendations into two major areas: Application and System Environment Controls; and Application and Business Processes Controls.

Approach

The approach for this engagement included:

- interviews with ministry management and staff;
- review of documents related to funding policies and procedures;
- preparation of a high-level process flowchart, and a detailed process flowchart with identified key controls;
- walkthrough and analysis of CDS processes and controls; and
- limited control and substantive testing as necessary.

Our fieldwork for this review was performed between March and May 2009.

Comments and Recommendations

Overall Conclusion

Overall, we concluded that the internal controls over transfer payments processing in CDS exist and are effective to ensure the integrity of the system.

We identified opportunities for the ministries to strengthen some of the internal controls over system security and to enhance business processes. Further information on our observations are included in the following sections of this report.

1.0 Application and System Environment Controls

CDS contains a set of security controls that address the Information Technology (IT) risks in the transfer payments process. These controls are both embedded in the application (e.g. audit trails) and are in place as operational processes (e.g. change management process).

We found there is no frequent downtime due to malfunction, malicious activity or side effects during the implementation of regular system changes. ***[Information withheld to protect security of a system].***

During our review, we identified opportunities to strengthen some of the system controls over CDS. More specifically, some changes are required to improve the process of CDS access request changes, ***[Information withheld to protect security of a system].*** The processes for ***[Information withheld to protect security of a system]*** and managing emergency changes should also be enhanced and/or documented.

1.1 Logical Security

Our objective was to assess whether logical security procedures are established to ensure only authorized users and IT Support staff have access to CDS financial functions and data in accordance with their roles.

We concluded that procedures are in place to allow only authorized users and IT support staff to have access to CDS, based on their role.

User accounts and passwords are currently required to access CDS. ***[Information withheld to protect security of a system].*** Also, CDS is set up to prevent the use of redundant User Ids. This security rule helps to track individual transactions and enforce accountability. CDS also has security mechanisms designed to prevent unauthorized access, undue activities, and record sensitive events to support after-the-fact investigations.

We identified that some CDS security features and related security processes could be enhanced to ensure the appropriate level of integrity and confidentiality of the information processed and stored in CDS.

Procedures on Access Request

An authorized logical access to CDS is required for each user to log-in to the system. Each logical access has a pre-defined role, based on business needs. We found that the CDS access request process is outlined in both FCB's and FAB's CDS Policy and Procedures manuals.

[Information withheld to protect security of a system].

Recommendations

(1) We recommend the ministries:

- **update the CDS Policy and Procedures Manual in order to detail the access request process of new accounts and changes in them; and**
- ***[Information withheld to protect security of a system].***

System Access Change/ Termination

When a systems access change or termination is required, FCB/FAB requests either a new access to CDS or a change to a user's current access. The Information & Technology Management Branch (ITMB) then implements the request

[Information withheld to protect security of a system].

Recommendations

(2) We recommend the ministries:

- ***[Information withheld to protect security of a system].***
- ***[Information withheld to protect security of a system].***
- ***[Information withheld to protect security of a system].***

[Information withheld to protect security of a system].

Recommendations

(3) We recommend ITMB:

- ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

[Information withheld to protect security of a system].

Recommendation

(4) ***[Information withheld to protect security of a system].***

Access to CDS Audit Information

CDS generates complete and sufficient audit records for relevant events, such as payment approval and generation of payments, which can support after-the-fact investigations of security incidents.

During the course of our review, we noted that the audit trail records are accessible through a specific CDS account by the following user groups: ***[Information withheld to protect security of a system].*** A clear role assignment on who has permission to access, modify and delete audit trails would enhance accountability and integrity of these records.

Recommendation

(5) ***[Information withheld to protect security of a system].***

1.2 Segregation of Duties

Our objective was to assess whether adequate segregation of duties is in place for the transfer payment process and system functions.

We concluded that sufficient segregation of duties is established for transfer payment process and system functions through the user profile. The CDS system security is "role-based". This characteristic enhances the overall security level of the system since different roles allow the user to access the different functions in the application. We also verified that:

- the application provides on-line reports describing the roles created and listing the active users according to their roles assigned;
- the basic rules regarding segregation of duties are described in Section 9.3.1 of the ministries' CDS Policy and Procedures Manuals; and
- the application is currently set up to prevent a transfer payment being created and authorized by the same person.

[Information withheld to protect security of a system].

Recommendations

(6) We recommend the ministries:

- ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

[Information withheld to protect security of a system].

Recommendation

(7) ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

- ***[Information withheld to protect security of a system].***

1.4 Change Management Process

Our objective was to assess whether formal change management procedures are in place to maintain the integrity of the CDS data and application.

We concluded that the change management process to manage and control changes to the computing environment, which includes CDS, exists and is adequate.

A tracking and reporting system ***[Information withheld to protect security of a system]*** is used to document the history and data of the CDS system fixes and enhancements. Regarding the CDS releases, we identified that the related documentation is available ***[Information withheld to protect security of a system].***

Procedures on Emergency Changes

The current Change Management Policy describes in detail the policies and procedures that ITMB should apply to manage and control changes to the computing environment. However this document does not describe the procedures to be followed in regard to emergency changes required for high priority changes. Having a formal process on emergency changes will ensure that a standardized approach for responding effectively to emergency changes is in place and that related risks are properly managed.

Recommendation

(8) We recommend ITMB review and update the current Change Management Policy to encompass the procedures for identifying, documenting, assessing, authorizing and recording emergency changes.

2.0 Application and Business Processes Controls

The application and business process controls include the governance structure applied through the Change Advisory Board (CAB); environmental controls applied primarily through the long standing experience of staff; and the controls embedded in the transfer payment process.

Oversight for CDS is provided by the ministries' CAB, which consists of the representatives from ITMB and key business areas. CAB monitors CDS and recommends any changes and enhancements on the system to the system owner. A monthly meeting is held to discuss any issues or enhancement opportunities related to CDS.

Most CDS users are those who were involved with the system implementation in 2005 and, as a result, most ministry staff generally have a good understanding of the system process and functionalities. We also reviewed the existing policy and other procedure manuals related to the transfer payment process. Key controls over the process were identified and necessary tests were performed by IAAS.

[Information withheld to protect security of a system].

Opportunities to formalize the risk assessment process and to implement system performance measures exist for the current CDS management process.

2.1 Roles and Responsibilities – End Users

Our objective was to assess whether roles and responsibilities over the transfer payments process and system functions are clearly defined and communicated.

Overall, we concluded that roles and responsibilities of FCB/FAB and FASB are clearly defined in the CDS Policy and Procedures Manual and other related procedure documents, and understood by ministry staff. CAB is also well recognized as the system management group to provide monitoring capacity, to both ministries, on CDS.

Changes in Organizational Structure and CDS System Governance

During our fieldwork, both ministries were in the process of changing their administrative and IM/IT organizational structure and, as a result, are working on redefining the governance structure of the CDS. Given limited resources in the current economic climate, having necessary business and technical support during this transition is critical to both ministries' CDS users to minimize any adversarial impact on operations. In the longer term when the organizational structure of each ministry is defined, the purpose, ownership and roles and responsibilities for the system management on risk, security and compliance should be confirmed by ministry management to maintain a clear accountability.

Recommendations

(9) We recommend the ministries:

- **In the short-term, ensure sufficient business and technical support is available during the transition for both FCB and FAB.**
- **In the long-term, ensure the following are confirmed and clearly defined:**
  - **the purpose of the system;**
  - **the ownership of the system; and**
  - **clear roles and responsibilities for the system management on risk, security and compliance.**

2.2 Management Monitoring

Our objective was to assess whether appropriate management monitoring controls and processes over transfer payments are in place.

We concluded that CAB is the key control in managing CDS and related transfer payment processes. An informal risk assessment process is used to identify potential risks and opportunities by CAB and that all mitigating actions are documented in a tracking system to monitor the progress.

Formalizing Risk Assessment Process

[Information withheld to protect security of a system]. A formal process will ensure that significant risks are monitored and acted upon on a timely basis. As well, a formal, periodic risk assessment with key stakeholders will ensure significant risks are identified and monitored.

Recommendation

(10) We recommend CAB establish a formal, periodic risk assessment with key stakeholders to ensure that:

- **risks are identified, assessed and documented;**
- **appropriate mitigating actions are defined and monitored; and**
- **responsibility is assigned to staff for each mitigating action.**

CDS System Performance Measures

We found that the existence of CAB is a good model of financial system governance to have a dedicated resource monitoring the system and be accountable to the system owner. We observed the opportunity for ITMB to further a good governance practice by implementing few technical key performance measures to demonstrate the effective and efficient management of the CDS and the related transfer payment processing. Some optional key performance measures for consideration are:

- percentage of successfully processed payment batches;
- expected level of system downtime;
- hours of unplanned downtime caused by operational incidents; and
- percent of scheduled work and requests not completed on time.

A balanced set of key performance measures will facilitate the continuous improvement on CDS by assisting decision making, improve performance and increase accountability through the collection, analysis and reporting of relevant performance-related data.

As a result, we suggest that ITMB establish a balanced set of few key performance measures, ensuring that these targets are specific, measurable, attainable, reliable and time-bound or SMART characteristics.

2.3 Policy and Procedures

Our objective was to assess whether ALMD and MED management has established policy and procedures related to transfer payments.

We concluded that the CDS Policy and Procedures, CDS Application Reference Manuals, and other related procedural documents have been sufficiently established for ministry staff for the roles and responsibilities and effective use of CDS and transfer payment processing.

2.4 Transaction Controls

Our objectives were to assess whether the attributes of integrity, authorization, reliability and availability of CDS output, application integrity and management trail do exist and related controls are effective.

We concluded that:

- Only authorized data is entered to the system.
- Payments are authorized by the appropriate authority. We also confirmed that the Authorization Audit Trail report can be extracted from the CDS system, which shows the description of what is being authorized down to the adjustment level, date and time, and the ID of who authorized it.
- Transactions can be traced back to CDS. We verified that the management trail structure is based on incremental record and its content provides enough information to support after-the-fact investigations of security incidents. Time stamps are also provided for use in audit record generation, which include "date" and "time" records.
- Necessary reconciliations are prepared and reviewed by the appropriate person in a timely manner, to ensure the completeness of processed transactions.

2.5 Compliance with Related Legislations in Regard to Timeliness of Payments

Our objective was to assess whether a process exists to monitor compliance with related legislation in regard to timeliness of payments.

We concluded that there is a process in place to monitor compliance with the related legislation in regard to timeline of payments for Public School Districts [*School Act*] and Independent Schools [*Independent School Act*].

The School Act requires each school district to be paid at least once a month. Currently, MED makes transfer payments twice a month to Public School Districts. With the authority in the *Independent School Act*, Grant Payments Order, Ministerial Order 37/04, requires eligible independent schools to be paid every quarter. The Office of the Inspector of Independent Schools has a separate system, Independent School Information System, to monitor quarterly payments.

The Library, University, and College and Institute Acts do not have any specific requirements for the timeliness of transfer payments.

Detailed Action Plan – Review of Common Disbursement System

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
1.0	**Application and System Environment Controls**				
1.1	**Logical Security**				
	1.	We recommend the ministries: • update the (CDS) Policy and Procedures Manual in order to detail the access request process of new accounts and changes in them; and • ***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].*** Once these processes are finalized, CDS Policy and Procedures Manuals will be updated and the new procedures communicated to users. • ***[Information withheld to protect security of a system].***	ITMB ITMB	Dec/09 Dec/09
	2.	We recommend the ministries: • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	ITMB ITMB ITMB	Dec/09 Dec/09 Dec/09

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
	3.	We recommend ITMB: • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].***	ITMB	Dec/09
	4.	***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].***	ITMB	Dec/09
	5.	***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].***	ITMB	Dec/09

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
1.2	**Segregation of Duties**				
	6.	We recommend the ministries: • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	ITMB/Ministry staff	Dec/09

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
[Information withheld to protect security of a system].					
	7.	We recommend the ministries: • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	• ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].*** • ***[Information withheld to protect security of a system].***	ITMB	Jan/10
1.4 Change Management Process					
	8.	We recommend ITMB review and update the current Change Management Policy to encompass the procedures for identifying, documenting, assessing, authorizing and recording emergency changes.	• ITMB will review and update the Change management policy as recommended	ITMB	Jan/10

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
2.0	**Application and Business Processes Controls**				
2.1	**Roles and Responsibilities – End Users**				
	9.	We recommend the ministries: • In the short-term, ensure sufficient business and technical support is available during the transition for both FCB and FAB. • In the long-term, ensure the following are confirmed and clearly defined: ➢ the purpose of the system; ➢ the ownership of the system; and ➢ clear roles and responsibilities for the system management on risk, security and compliance.	• Ministries continue to work together to exercise the roles and responsibilities in a seamless manner to ensure there is no impact on the operations at all. Roles and responsibilities are defined and confirmed in the CDS Policy and Procedures Manual and other related procedure documents. These are clearly understood by relevant ministry staff. ITMB continues to ensure security assessments, compliance assessments, and risk assessments are carried out and complete support is available. It is endeavoured that controls, including compensatory controls are in place. CAB regularly and closely monitors all processes and provides governance. In the long run the purpose, ownership and roles and responsibilities, including Terms of Reference for CAB, will be re-visited and where necessary will be confirmed and defined by the ministry management to clarify the accountability.	CAB/Ministries Executive & SFO's	In the long run, it's an on-going process. Next review by October 2010

Priority	Rec. #	Recommendations	Management Comments to be Included in Report (Action Planned or Taken)	Assigned To	Target Date
2.2	**Management Monitoring**				
	10.	We recommend CAB establish a formal, periodic risk assessment with key stakeholders to ensure that: • risks are identified, assessed and documented; • appropriate mitigating actions are defined and monitored; and • responsibility is assigned to staff for each mitigating action.	• CDS will be assessed regularly according to current ministry standards in Risk Assessment, Security, and Financial Controls. In addition CAB will document and assess any risk presented to the committee. Request for this audit was one of the strategies to assess risks associated with CDS. • ITMB maintains a list of any immediate and long-term CDS systems issues. This list is reviewed monthly at CAB.	ITMB, CAB	ongoing