Employment and Social Development Canada | Emploi et Développement social Canada

Now and Tomorrow, Excellence in Everything We Do

Protected A

Internal Audit Services Branch

Audit of the Departmental Information System and Technology Controls – Phase 1– Application Controls

November 2014

SP-1084-01-15E

Canada

You can download this publication by going online: http://www12.hrsdc.gc.ca

This document is available on demand in multiple formats (large print, Braille, audio cassette, audio CD, e-text diskette, e-text CD, or DAISY), by contacting 1 800 O-Canada (1-800-622-6232).

If you use a teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No.: Em20-22/2015E-PDF
ISBN/ISSN: 978-1-100-25532-3

Table of Contents

Executive Summary

Information Technology (IT) General Controls (ITGCs) are a set of control activities established within the IT environment that can be applied to every system, application, process, and set of data files that the Department relies on for decision-making in its day-to-day operations. ITGCs are established to ensure the adequate development and implementation of applications, in addition to the integrity of programs, data files, and computer operations. ITGCs create the IT environment where the applications function and consist of two types of controls, general controls and application controls.

General controls (or ITGCs) include access controls, backup and recovery controls, and computer operation controls. Application controls, which are specific to computer programs, include controls over accuracy and completeness of data inputs, data outputs, validity of transactions, and reporting. ITGCs and application controls fall under the overarching umbrella defined as the Departmental Information System and Technology Controls (DISTCs).

Employment and Social Development Canada (ESDC) has over 300 applications which staff use on a day-to-day basis to perform operational activities. A series of criteria were used to assess these 300 applications in order to determine which applications to select for this audit. Furthermore, since the Office of the Auditor General (OAG) in its Report on the Public Accounts assesses on an annual basis ITGCs for ESDC's two important statutory programs (Employment Insurance (EI), and the Canada Pension Plan (CPP)); the general controls that directly support these major programs were not part of our assessment. The applications selected were based on whether the application met the following criteria:

- Serves more than one program;
- Is in production;
- Is developed in-house or heavily customized;
- Has a high impact on the delivery of a particular program(s);
- Is subject to complex changes;
- Is not planned for replacement in the near future;
- Has a high volume of transactions or activities;
- Has significant financial impacts; and
- Has an impact on Canadians.

Based on the selection criteria and initial risk assessment conducted, the following three systems were selected for this audit:

- Departmental Accounts Receivable System (DARS)
- Common System for Grants and Contributions (CSGC)
- Social Insurance Number – Social Insurance Registry (SIN-SIR)

Audit Objective

The objective was to assess the adequacy of the DISTCs for the applications scoped in Phase 1 of the audit.

Summary of Key Findings

- Processing systems/automated controls are adequately designed and operating effectively to ensure that transactions are processed as intended, are accurate, and are timely.

- When systems are planned, designed and programmed, logical access measures and controls are considered to prevent unauthorized access, modification, or disclosure of system data. PROTECTED.

- Backups are repeatedly and systematically performed. The Department, however, does not have a clear and written Service Level Agreement (SLA) or Memorandum of Understanding (MOU) with Shared Services Canada (SSC). In addition, backups of system data are not periodically tested for accuracy and completeness putting the Department at risk of not having complete records of the "last known good copy" of its system data.

- Output systems/automated controls are adequately designed and operating effectively to ensure that transactions are processed as intended, are accurate, and are timely.

- All three applications have an audit trail and audit log files are maintained, PROTECTED.

Audit Conclusion

The audit concluded that the Department has adequately designed the automated application processing controls for the departmental information systems scoped in. However, the areas for improvement noted in this audit for **PROTECTED** backups are, in our opinion, necessary to further enhance and strengthen the IT controls in place to ensure that the DISTCs operate as intended.

Recommendations

- Innovation, Information, and Technology Branch (IITB), in collaboration with the application business owners for DARS (Chief Financial Officer Branch or CFOB), CSGC (Program Operations Branch or POB), and SIN-SIR (Integrity Services Branch or ISB), should have a clear and written SLA or MOU with SSC that defines roles and responsibilities with respect

to the creation and management of backups. Specifically, IITB should determine with SSC who is responsible and accountable to test the backups produced by SSC to ensure they are complete and available in the event data is required to be restored.

- PROTECTED

1.0 Background

1.1 Context

ITGCs are a set of control activities established within the IT environment that can be applied to every system, application, process, and set of data files that the Department relies on for decision-making in its day-to-day operations. ITGCs are established to ensure the adequate development and implementation of applications, in addition to the integrity of programs, data files, and computer operations. ITGCs create the IT environment where the applications function and consist of two types of controls, general controls and application controls.

General controls (or ITGCs) include access controls, backup and recovery controls, and computer operation controls. Application controls, which are specific to computer programs, include controls over accuracy and completeness of data inputs, data outputs, validity of transactions, and reporting. ITGCs and application controls fall under the overarching umbrella defined as the DISTCs.

ESDC has over 300 applications which staff use on a day-to-day basis to perform operational activities. A series of criteria were used to assess these 300 applications in order to determine which applications to select for this audit. Furthermore, since the OAG in its Report on the Public Accounts assesses on an annual basis ITGCs for ESDC's two important statutory programs (EI and CPP); the general controls that directly support these major programs were not part of our assessment. The applications selected were based on whether the application met the following criteria:

- Serves more than one program;
- Is in production;
- Is developed in-house or heavily customized;
- Has a high impact on the delivery of a particular program(s);
- Is subject to complex changes;
- Is not planned for replacement in the near future;
- Has a high volume of transactions or activities;
- Has significant financial impacts; and
- Has an impact on Canadians.

1.2 Audit Objective

The objective of this engagement was to assess the adequacy of the DISTCs for the applications scoped in Phase 1 of the audit.

1.3 Scope

The work was conducted under the umbrella of DISTCs based on a phased approach; which will span over the next few years.

A series of criteria, outlined in Section 1.1, was used in selecting the applications and related key interfaces to test.

The first phase of the DISTCs Audit focused on selected application and general controls associated with the SIN-SIR, DARS, and the CSGC and their selected key interfaces. Appendix C provides an overview of the applications and related interfaces that were chosen.

Since IITB is currently implementing the Management Action Plan (MAP) developed in response to the Gartner Information Security Program Assessment Report, components of the Gartner report were not included in this audit. Furthermore, Internal Audit Services Branch (IASB) will be initiating an IT security assessment to provide a snapshot view and to report trends of the IT security posture in the Department. This will determine and assess risk areas, including the identification of gaps and overlaps, taking into consideration what have already been covered in recent audits, reviews and assessments to determine future audit direction. Also, IASB has planned engagements that will be performed in subsequent years, as per the commitments made in the context of the IT Security Audits.

1.4 Methodology

The DISTCs, Phase 1 audit was conducted using a number of methodologies which included interviews, walkthroughs of business process, control questionnaires, control testing, as well as a review and analysis of process flow charts, maps, and documentation.

Process maps were also prepared for CSGC and DARS regarding their inputs into the departmental financial statements.

The audit fieldwork was conducted between June 2014 and September 2014.

2.0 Audit Findings

The following presents strengths and opportunities for improvement as they relate to DISTCs.

2.1 Data is processed accurately and in a timely manner

Data input controls are important as they ensure the accuracy, completeness, and timeliness of data during its input, transfer or conversion from its original source into a computer application. Data can be entered into a computer application from either manual online input or by batch processing (automated). When reviewing input controls it is important to determine the adequacy of both manual and automated controls over data input to ensure the accuracy of data input with optimum use of computerized validation and editing. It is also important that error handling procedures facilitate the timely and accurate resubmission of all corrected data. Based on our audit testing we found that data input controls for DARS, CSGC, and SIN-SIR are operating effectively.

When data is interfaced into DARS, CSGC, and SIN-SIR the system automatically checks the batch file to ensure it contains the correct sequence number. For example, validation checks are in place so that a batch being processed has a sequence number that is sequential to the last batch processed. In addition, there is an annual reconciliation conducted by ESDC staff in the Bathurst, New Brunswick office with data from the CPP application system to ensure data transferred from the program is consistent with that in SIN-SIR. Field input controls are also in place (e.g. set # of digits per field, SIN number verification, alpha-characters only, numeric data only, segregation of duties in CSGC, pre-populated tables and drop-down menus, etc.).

For the DARS interface with Canada Student Loans Program (CSLP) system, interest rates are pre-set into the system so users do not have the ability to change rates. Rates are entered in DARS by Financial Systems staff who do not have the ability to modify or approve transactions in DARS. These rates are only changed when the program area (e.g. CSLP) notify them of a change in rate.

Quality Control reports are produced by all three systems for batch processing in order to detect and identify abnormalities. These reports are reviewed by the respective application's Quality Assurance team following each batch run. In addition to file sequences used for data validation, the application will check headers[1] for source identification and trailers[2] to confirm record counts. For DARS, Quality Control reports also contain a hash total[3] which verifies the sum of a particular field for all the data transferred and compares it to the same hash total of the input file prior to input into DARS.

1 Headers are information structures which identify the information that follows, such as a block of bytes in communication flow.

2 Trailer is the information which occupies several bytes at the end of the block of the data being transmitted. Headers and trailers contain error-checking data which is useful for confirming the accuracy and status of the transmission.

3 A method for ensuring the accuracy of processed data. It is a total of several fields of data in a file, including fields not normally used in calculations, such as account number. At various stages in the processing, the hash total is recalculated and compared with the original. If any data has been lost or changed, a mismatch signals an error.

With respect to a rejected transaction, such as a failed electronic validation (e.g. wrong SIN# interfaced from the CSLP application system and Provincial Vital Events database), Bathurst agents perform a manual verification of the data onscreen to ensure data transferred from CSLP to SIN-SIR is accurate. These online screens contain various edit checks for invalid entries and display error messages. Further, the online screen will also prompt agents to double check the information entered to ensure that no data capture errors have occurred before continuing.

All three systems also have adequate controls around segregation of duties. For example in DARS a user cannot have a profile that allows the user to both modify and approve a transaction. Similarly in CSGC, there are automated application controls that prevent a user from having both data entry and approval profiles.

As a result, based on the controls tested for processing we conclude that automated controls are adequately designed and operating effectively to ensure that transactions are processed in an accurate and timely manner.

2.2 Controls related to PROTECTED backups need to be strengthened

PROTECTED

Backups

The primary purpose of maintaining backups is to recover data after its loss, be it by data deletion or corruption or even a disaster. Data loss can be a common experience of computer users or applications, and as a result requires effective disaster recovery and business continuity planning controls. To ensure that the backup process is reliable and working as expected, regular backup testing should be conducted.

There are advantages to conduct backup testing. Firstly, backup testing allows data integrity to be verified without reference to the original file. Secondly, backup testing can also help to avoid making redundant copies of files, and thus improve backup speed. Many organizations rely on third-parties to test, validate and optimize their backup operations.

During the course of this audit, it was determined through interviews that all three selected applications are following standard backup procedures, especially when it comes to the frequency of the file synchronization process. ESDC currently relies on SSC to conduct its backup operations for DARS, CSGC, and SIN-SIR. Based on interviews conducted, it was found that ESDC used backups in the past to selectively fix problems with regards to the three application systems; however, it has not had to perform a full database recovery. The ability to recover a full database of any of these three systems has yet to be tested.

In addition there is no MOU or SLA between ESDC and SSC with respect to the backup services provided by SSC, however, SLAs in place before SSC was created are being honoured. Having a SLA or MOU will facilitate the understanding of the roles and responsibilities with respect to the creation and management of backups so that ESDC can ensure adequate backup controls are in place.

A full backup is created for DARS daily. Each week, information from the daily backups is compiled and stored in another database. Before each new release or update of DARS, a separate backup is taken in case anything occurs to the system as a result of the update.

For CSGC, data backups for the Labour Market Development Agreements (Web LMDA) application system and DARS interface are handled by SSC who conducts daily backups. CSGC also keeps a backup of the batch file it sends into DARS through its DARS batch file for four weeks. In addition CSGC conducts quality checks once all files are processed to ensure the data is adequately backed up.

For SIN-SIR, its data is hosted on the PROTECTED. In this case, PROTECTED is responsible for the data integrity and data recovery services.

Recommendation

IITB, in collaboration with the application business owners for DARS (CFOB), CSGC (POB), and SIN-SIR (ISB), should have a clear and written SLA or MOU with SSC that defines roles and responsibilities with respect to the creation and management of backups. Specifically, IITB should determine with SSC who is responsible and accountable to test the backups produced by SSC to ensure they are complete and available in the event data is required to be restored.

Management Response

IITB doesn't agree that we should have SLAs in place for details as finite as backups per application – the task involved in both initially creating and then maintaining such level of detail in SLAs is prohibitive. However, we are working on strengthening rigor. IITB is in process of developing an Operating Protocol that will outline where MOUs and SLAs are required; the expected level of operational performance as well as escalation procedures. The estimated completion date is March 31, 2015.

2.3 Output controls are adequately designed and operating effectively

Data output controls are used to ensure the integrity of data outputs and the accurate, complete and timely dissemination of any output produced. Outputs can be in hardcopy form, in the form of files used as input to other systems, or information available for online viewing. Output controls were evaluated to assess the adequacy of controls over outputs to ensure that the data processing results are accurate and reliable, output control totals are accurate and are being verified, and the resulting information is distributed in a timely and consistent manner to the end users.

DARS generates financial information and outputs it through the Decision Support System (DSS) interface which receives the financial information for purposes of preparing the Department's financial statements and public accounts reports. Similar to the output controls for CSGC, batch files outputted from DARS to DSS go through an automatic data validation process. DARS checks the sequence number to ensure it follows the proper sequence in addition to validating the record and hash totals prior to processing.

CSGC outputs information on any overpayments, or amounts owing from clients, into DARS via a batch file output. The batch file output into DARS goes through an automatic data validation process. CSGC checks the sequence number to ensure it follows the proper sequence in addition to validating the record and hash totals prior to processing. Other outputs are real-time generated, for example, CSGC and web-LMDA, and as such do not require any control over interfaced files.

For SIN-SIR, if there are issues with particular transactions, data can be re-sent for validation by the CSLP system, or individual SINs can be validated and re-extracted from the CPP system.

For all three applications Quality Control reports are also produced to show record counts of data extracted to validate that the data output is complete. In addition, all three applications conduct automated validation checks[4] to ensure that a batch being processed has a sequence number that is sequential to the last batch processed.

2.4 Audit trails are maintained, PROTECTED

An audit trail is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities. Audit records result from activities or transactions that are processed through applications. Audit trails can capture all the information related to a particular entry, modification, creation, deletion, etc. of a transaction in a particular application.

4 Data validation is the process of ensuring that an application operates on clean, correct and useful data.

All SIN access and updates to accounts are recorded in an online audit trail maintained by the SIR application. The audit trail PROTECTED is used for investigation purposes. PROTECTED

PROTECTED

For DARS an audit trail is maintained for transactions completed within DARS. PROTECTED they can be used for investigation purposes. PROTECTED

For CSGC, all screens that a user enters are tracked in addition to all the SIN accounts looked up. The audit trail retains such information to be used in the event of an investigation, PROTECTED

PROTECTED

Recommendation

PROTECTED

Management Response

The ADM, ISB agrees with this recommendation and will engage with partners and undertake the necessary analysis PROTECTED. Actions are expected to be completed by September 2015.

3.0 Conclusion

The audit concluded that the Department has adequately designed the automated application processing controls for the departmental information systems scoped in. However, the areas for improvement noted in this audit for PROTECTED backups are, in our opinion, necessary to further enhance and strengthen the IT controls in place to ensure that the DISTCs operate as intended.

4.0 Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the assessment of DISTCs for the scoped in interfaces of the DARS, CSGC, and SIN-SIR. The evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*.

Appendix A: Audit Criteria Assessment

PROTECTED

Appendix B: Glossary

CFOB	Chief Financial Officer Branch
CPO	Chief Privacy Officer
CPP	Canada Pension Plan
CRA	Canada Revenue Agency
CSGC	Common System for Grants and Contributions
CSLP	Canada Student Loans Program
DARS	Departmental Accounts Receivable System
DARSCOM	DARS Inter-System Communication Interface
DISTCs	Departmental Information System and Technology Controls
DSS	Decision Support System
EI	Employment Insurance
ESDC	Employment and Social Development Canada
IASB	Internal Audit Services Branch
IITB	Innovation, Information, and Technology Branch
ISB	Integrity Services Branch
IT	Information Technology
ITGC	Information Technology General Controls
ITRDS	Information Technology Renewal Delivery System
LMDA	Labour Market Development Agreements
MAP	Management Action Plan
MITS	Management of Information Technology Security
MOU	Memorandum of Understanding
OAG	Office of the Auditor General
POB	Program Operations Branch
SAP	System, Applications & Product
SIN	Social Insurance Number
SINRA	Social Insurance Number Rapid Access
SIN-SIR	Social Insurance Number – Social Insurance Registry
SLA	Service Level Agreement
SSC	Shared Services Canada

Appendix C: Selected Applications and Interfaces Overview

SIN-SIR

The SIN-SIR plays a crucial role in the operation of programs including the EI, CPP, Old Age Security, and CSLP. It contains information on each person who has been issued a SIN, including information provided on the original application by the client. SIR keeps records on name changes, other amendments, applications for replacement cards and special account information.

Interfaces associated with SIN-SIR were reviewed against the criteria listed on page 4 of this report in order to determine which ones would be included in the audit scope. As a result, application controls of the SIN-SIR and its key interfaces with CSLP, CPP, Vital Events, and SIN Rapid Access (SINRA) web application, that give agents in local offices the ability to serve customers using custom built web pages to access the SIR, were reviewed during the conduct phase of the audit.

DARS

The Department has many programs which generate accounts receivable, such as EI, CPP, and CSLP. DARS is a generic, national, online system, designed to store and manage various types of accounts receivable within the Department. Through interface systems, DARS collects account information related to various statutory programs including CPP overpayments, EI overpayments, and penalties. The DARS was built on the concept of one client with potentially many accounts, and with one Recovery Officer responsible for recovering the client's debt. The DARS is also used to perform accounting functions on defaulted Canada Student Loans accounts and other accounts receivable. The DARS operates with PROTECTED *and is managed by CFOB.*

Interfaces associated with DARS were reviewed against the criteria listed on page 4 of this report in order to determine which ones would be included in the audit scope. Application controls of DARS and its key interfaces, namely CPP (Information Technology Renewal Delivery System (ITRDS)), CSLP, DARS Inter-System Communication Interface (DARSCOM), and DSS were examined during the conduct phase. Interfaces with the Canada Revenue Agency (CRA) and System, Applications & Product (SAP) will not be in scope. Because of the early stage of the SAP implementation and the development of an interface between SAP and DARS, the testing of the latter will be done in future audits.

CSGC

The CSGC is an internally-developed, bilingual application to administer departmental grants and contributions programs. The CSGC was launched across the Department in the third quarter of 2001 and operates on an Oracle platform. The system enables users to electronically document all phases of the project life cycle from application to close-out and to manage individual client cases. The CSGC has introduced a reporting capability that also allows users to generate a variety of reports on the Department's recipient base and the projects for which these recipients are funded. The CSGC is managed by the Transaction Processing Portfolio from IITB. The system currently processes approximately two billion annually in grants and contributions (2010-11 estimates) managed through Regional offices and POB.

Interfaces associated with CSGC were reviewed against the criteria listed on page 4 of this report in order to determine which ones would be included in the audit scope. Application controls of CSGC as well as key interfaces including DARS and Web LMDA were examined during the conduct phase. External interfaces with CRA and Public Works and Government Services Canada were not included in the audit scope.