Statistics Canada   Statistique Canada

Audit Report

Audit of Research Data Centres Universities Calgary and Lethbridge

December 2011

Project Number: 80590-66

Canada

Table of Contents

Executive Summary 1

Introduction 3

Background 3

Audit Objectives 4

Scope 4

Approach 4

Authority 4

Findings, Recommendations and Management Response 5

Administration of Microdata Research Contracts and Disclosure Risk Analysis 5

Physical Security 10

Information Technology Security 12

Appendix 15

Appendix A: Audit Criteria 15

Executive Summary

The Prairie Regional Research Data Centres (RDCs) consist of a main laboratory located in the McKimmie Library, University of Calgary, (the host centre), and at the University of Lethbridge, (the branch centre). It provides services to approximately 122 researchers working on an average of 51 projects a month. University researchers have access to 191different Statistics Canada datasets in the Centre.

The security measures that are implemented in the Prairie Regional RDCs must safeguard the confidentiality of the data to the same degree as in the Statistics Canada offices.

The objectives of the audit are to provide the Chief Statistician and the Departmental Audit Committee with assurance that the RDCs at the University of Calgary and University of Lethbridge:

- Have effective practices and mechanisms in place to ensure that the confidentiality of data is protected in the delivery of services.
- Comply with applicable Treasury Board of Canada Secretariat (TBS) and Statistics Canada policies and standards regarding Information Technology (IT) and Physical Security, to ensure that confidentiality of data is protected in the delivery of services.

The audit was conducted by Internal Audit Services in accordance with the Government of Canada's *Policy on Internal Audit.*

Key Findings

Roles, responsibilities, and accountabilities are defined and communicated in the following areas: Administration of Microdata Research Contracts (MRCs), disclosure risk analysis, physical security and information technology (IT) security at the RDCs. Authority is formally delegated at the program and operations level. Processes and procedures for disclosure risk analysis are in place and requests for disclosure risk analysis are carefully administered and screened by the RDC analyst to ensure that confidentiality of data is not compromised. Applicable physical security measures and IT access, identification and authentication safeguard measures are in place and adhered to for safeguarding and protecting Statistics Canada confidential data. Access to the Prairie Regional RDCs is restricted to authorized personnel, i.e. deemed employees, such as researchers and university IT support staff.

The audit noted that access into the RDCs and access to microdata files is provided to researchers before security clearance is received from Departmental Security (DS) and misunderstanding exists between the RDC program and DS on the procedure for handling classified security clearance forms and monitoring of security clearances. The audit revealed that operational efficiencies could be optimized by improving the management and inventorying of administrative information on research projects at the Microdata Access Division (MAD) Head Quarters (HQs).

The assessment of the system and communications' protection safeguards revealed that opportunities exist to strengthen the computing environment by ensuring that all Universal Serial Bus (USB) ports on all stand-alone workstations are disabled and by reducing the login timeout of the workstations.

Overall Conclusion

Physical security measures and IT access, identification and authentication safeguard measures are compliant with applicable TBS and Statistics Canada policies and standards. Processes and procedures for disclosure risk analysis are in place and requests for disclosure risk analysis are carefully administered and screened by the RDC analyst to ensure that confidentiality of data is not compromised.

The audit results highlighted opportunities for improving the practices and mechanisms that are in place to ensure that confidentiality of data is protected in the delivery of services. Areas to be strengthened are: 1) Disabling USB ports and reducing the login timeout on the stand-alone workstations. 2) Access into the RDCs and access to microdata files should be provided to researchers only after receiving security clearance from DS. 3) Consultation with DS to obtain clarity on the procedure for handling classified security clearance forms and monitoring of security clearance. 4) Optimize operational efficiencies by improving the management and inventorying of administrative information on research projects at the MAD HQ.

Conformance with Professional Standards

The conduct of this engagement conforms to the International Standards for the Professional Practice of Internal Auditing and the Government of Canada Internal Auditing Standards. Sufficient testing was carried to support the findings and related recommendations.

Patrice Prud’homme
Chief Audit Executive
Internal Audit Services, Statistics Canada

Introduction

Background

Decision-makers need an up-to-date and in-depth understanding of Canadian society to help them respond not only to today's needs, but to anticipate tomorrow's as well. This need is underlined by a growing demand for analytical output from the rich sources of data collected by Statistics Canada.

In 1998, the Canadian Initiative on Social Statistics studied the challenges facing the research community in Canada. One of the recommendations of the national task force report on the *Advancement of Research using Social Statistics*, was the creation of research facilities to give academic researchers improved access to Statistics Canada's microdata files.

The RDCs are part of an initiative by Statistics Canada, the Social Sciences and Humanities Research Council (SSHRC), Canadian Institutes of Health Research (CIHR) and university consortia to strengthen Canada's social research capacity and to support the policy research community. The SSHRC is the federal agency that promotes and supports university-based research and training in the social sciences and humanities. CIHR is the major federal agency responsible for funding health research in Canada.

Twenty-four RDCs are located in a secure setting on university campuses and provide researchers with access to microdata from population and household surveys. Researchers do not need to travel to Ottawa to access Statistics Canada microdata. There is also a Federal Research Data Centre in Ottawa which provides microdata access to researchers from federal policy departments.

The Prairie Regional RDC opened in 2001 and is located in the campus library building at the University of Calgary. It is a full-time medium size facility with 14 workstations available for researchers to conduct their research, Monday to Friday between 8:30 to 4:30. It is staffed by one full-time and one part-time Statistics Canada analyst. In October 2010, a Branch RDC was inaugurated in the campus library building of the University of Lethbridge. All new RDC sites begin as Branches of an existing Centre and remain as Branches until the level of activity warrants consideration as a full Centre. The Branch RDC is staffed by a part-time Statistics Canada statistical assistant who is responsible for maintaining security when the facility is open part-time for 12.5 hours a week, and working in cooperation with the host University of Calgary analysts.

The Prairie Regional RDCs are operated under the provisions of the *Statistics Act* in accordance with all the confidentiality rules and are accessible only to researchers with approved projects and who have been sworn in under the *Statistics Act* as deemed employees.

Audit Objectives

The objectives of the audit are to provide the Chief Statistician and the Departmental Audit Committee with assurance that the RDCs at the University of Calgary and University of Lethbridge:

- Have effective practices and mechanisms in place to ensure that the confidentiality of data is protected in the delivery of services.
- Comply with applicable TBS and Statistics Canada policies and standards regarding Information Technology and Physical Security, to ensure that confidentiality of data is protected in the delivery of services.

Scope

The scope of this audit included an examination of the systems and practices of the Prairie Regional RDCs at the University of Calgary and University of Lethbridge in the protection of data, use of technology and the physical security.

The audit focused on disclosure risk analysis and vetting of data output by the on-site Statistics Canada employees; deemed employee status and security clearance requirements for access to microdata; research proposal process for RDC; microdata research contract; physical security of the RDC sites in compliance with applicable TBS and Statistics Canada policies and standards; and IT protection in compliance with applicable TBS and Statistics Canada policies and standards.

Approach

The field work was performed in two stages: the first stage consisted of a review and assessment of the processes and procedures to ensure physical security, use of technology, and the protection of data. The second stage consisted of site visits to the Prairie Regional RDCs to test controls for safeguarding microdata files including logical access and computer security controls, and to perform compliance testing of the centres to assess the physical security measures in place.

Authority

The audit was conducted under the authority of Statistics Canada Multi-Year Risk-Based Audit Plan 2011/12-2013/14, approved March 2011 by the Departmental Audit Committee.

Findings, Recommendations and Management Response

Line of Enquiry #1: Research data centres have effective practices and mechanisms in place to ensure that the confidentiality of data is protected in the delivery of services at the regional research data centre.

Administration of Microdata Research Contracts and Disclosure Risk Analysis

The authority required for the administration of the MRCs and disclosure risk analysis is formally delegated at the program and operations level and roles and responsibilities are defined and communicated.

Processes and procedures for disclosure risk analysis are in place and requests for disclosure risk analysis are carefully administered and screened by the RDC analyst to ensure that confidentiality of data is not compromised.

Operational efficiencies could be optimized by improving the management and inventorying of administrative information on research projects at the MAD HQs. Access into the RDC and access to microdata files is provided to researchers before security clearance is received from DS. Misunderstanding exists between the RDC program and DS on the procedure for handling classified security clearance forms and monitoring of security clearances.

Administration of Microdata Research Contracts

Administration of Microdata Research Contracts (MRCs) i.e. controlling and protecting designated information held in RDCs; establishing and maintaining an inventory of administrative information on research projects; and ensuring that access to RDCs is only granted to researchers with valid security clearances is a combination of assigned responsibilities, procedures, and controls used to effectively manage MRCs and ensure data confidentiality.

Authority

RDCs operate under the provisions of the *Statistics Act* in accordance with all the confidentiality rules and are accessible only to researchers with approved projects who have been sworn in under the *Statistics Act* as “deemed employees”.

Roles and Responsibilities

Roles and responsibilities for the management of the MRCs, access to confidential microdata and disclosure risk analysis are defined and communicated to all the stakeholders in policies, standards, procedures documents and detailed guides. At the program level, authority is formally delegated to the RDC Program Manager in Statistics Canada’s *Security Practices Manual*, which requires *"certification that required procedures for administrative information…research proposal and other information throughout the life-cycle of the project, have been followed"*. The audit noted that the "certification" process is not defined and there is ambiguity within the RDC Program as to what exactly is meant.

Contract Processing Procedures

A research project starts with the RDC analyst determining the data access needs. If access to a RDC is the appropriate data access route, the researcher then prepares a proposal for data access with the assistance of the RDC analyst, if required. This proposal is submitted on-line to SSHRC. The proposal undergoes a peer review where the proposal is assessed on its academic merit and an institutional review by Subject Matter Area to determine if analytical data is needed and whether the data can support the project. On receipt of notification of approval of the project from the Microdata Access Divison at Head Quarters, the RDC analyst draws up the contract for the researcher(s) to sign and invites the researcher(s) to an orientation session and to sign the contract. At the orientation session, training on strategies for disclosure risk analysis, Information Technology and physical security measures is provided to the researcher(s). The *Researcher's Guide* which describes researchers' and RDC analysts' roles and responsibilities in the RDC and Statistics Canada's *Values and Ethics Code for the Public Service* are provided to the researchers, who acknowledge their receipt by signing for the documents.

The audit tested compliance of the contract processing procedures by reviewing a sample of randomly selected contracts which included 21 of 182 contracts (11%) as of December 2010, for the Prairie Regional RDCs. The audit noted that for 20 contracts, records of the project proposal with a listing of the data sets, the project approval email and signed copies of the MRC and its respective amendments and revision(s) were on file and were complete. Documentation for one contract could not be located because it had not originated at the Prairie RDC.

As "deemed employees", the researchers are required to undergo a reliability security screening pursuant to sub-sections 5(2) and 5(3) of the *Statistics Act,* and take an oath or affirmation of office and secrecy, pursuant to sub-section 6(1) of the *Statistics Act.* The audit determined that the security forms are completed and the oath of office is taken when the researcher(s) sign the MRC. The original security forms are forwarded by courier by the RDC analyst to MAD HQ, for submission to Departmental Security (DS) for processing. However, from our sample of 21 contracts, representing 37 researchers, only 7 out of 37 copies of the signed oath and 13 out of 37 security clearance documents could be located by MAD HQ for our review.

Access into the RDC and data access should be granted to the researchers by the RDC analyst on receipt of email from MAD HQ on the security clearance start and end dates issued by DS. This is per the procedures document *"Conducting Security Clearance Procedures for RDC researchers"* prepared by MAD, which was confirmed with DS. The audit revealed that at the Prairie Regional RDCs access into the RDCs and to the data begins immediately for any researcher who submits completed documentation for security clearance but does not indicate having a criminal record. Request for disclosure risk analysis however, is only allowed when the RDC analyst receives an email from MAD HQ on the security clearance start and end dates issued by DS. This conflicting direction is provided in a presentation *Security Clearance – Flow of Information*, prepared by MAD HQ.

The audit also noted that the procedures document *"Conducting Security Clearance Procedures for RDC researchers"* is not consistent with the direction and understanding of DS with regards to the proper handling of classified security clearance documents and the appropriate date for monitoring security clearances. As a result, misunderstanding exists between MAD HQ, the RDC analyst and DS. This increases the risk of incorrect practices being followed and wrong decisions being made. Also there is no directive on the retention period for original security clearance documents specific to the RDC program.

There is no directive on the retention period for researchers' archived folders specific to the RDC program (i.e. zipped, encrypted and put on compact discs or external hard drives; and the hard copy files of the researchers' disclosure risk analysis). Archived information dating back to when the University of Calgary RDC opened is stored in locked cabinets in the secured server room and in the locked workstation cabinets.

Recommendations:

It is recommended that the Assistant Chief Statistician Social, Health and Labour Statistics Field ensure that:

- *Clarity on the "certification process" specified in the* Securities Practices manual *is provided.*
- *Complete files for the MRCs including copies of the security clearance documents and signed oaths by deemed employees are maintained at HQ.*
- *In consultation with DS, provide clarity by updating the procedures document "Conducting Security Clearance Procedures for RDC researchers" for the following:*
  - ✓ *Responsibilities of the RDC analyst and HQ on the handling of the original security clearance documents.*
  - ✓ *Procedures on when access to the RDC is to be granted to a researcher and when a researcher can request disclosure risk analysis for removing information from the RDC.*
  - ✓ *Procedures on the end date to be monitored by HQ for security clearance for Canadian and foreign students (imbed a "Print screen" of Client Relations Management System security information field and highlight the "end date" to be monitored by HQ staff).*
  - ✓ *Retention period for the original security screening documents by HQ.*
- *Guidance on the retention period for archived material and researchers' hard copy files is provided.*

Management Response:

Management agrees with all of the recommendations.

- The Manager, MAD has ensured that the documentation for the program has been reviewed and the recommended changes have been made to clarify the “certification process”. The changes have been communicated to all analysts working in the RDCs.

  Deliverable and Timeline: Update to the procedures document *“Conducting Security Clearance Procedures for the RDC researchers”*completed.

- The Manager, MAD has ensured that the filing structure to improve the timeliness for retrieving hard copy historical information has been modified and that all information will be filed under the principle investigator’s name.

  Deliverable and Timeline: Modified filing structure at MAD HQ, by March 31, 2012.

- The Manager, MAD has ensured that DS has been consulted to provide clarity in the procedures document *“Conducting Security Clearance Procedures for the RDC researchers”* with respect to:
  - The responsibilities of the RDC analyst and HQ on the handling of the original security clearance documents.

    Deliverable and Timeline: Update by December 31, 2011.

  - Procedures on when access to the RDC is to be granted to a researcher and when a researcher can request disclosure risk analysis for removing information from the RDC.

    Deliverable and Timeline: Update to the procedures document completed, and understanding by the RDC analysts confirmed.

  - Procedures on the end date to be monitored by HQ for security clearance for Canadian and foreign students.

    Deliverable and Timeline: Print screen in the procedures document included.

  - Retention period for the original security screening documents by HQ has been clarified with DS.

    Deliverable and Timeline: Update the *“Internal Operations Guide”* by March 31, 2012.

- The Manager, MAD has ensured that the RDC managers have met with Information Management Division to provide input into the *Directive on Archiving and Retention Periods*.

  Deliverable and Timeline: Implementation plan for archiving RDC files by March 31, 2012.

Disclosure Risk Analysis

RDCs are repositories of Statistics Canada master microdata files that are accessible to researchers with approved projects. Effective and appropriate processes and procedures for disclosure risk analysis should be in place and adhered to in order to significantly reduce the risk of unwanted disclosure. Requests for disclosure risk analysis should be carefully administered and screened by the RDC analyst, as per the established protocols, to ensure that confidentiality of data is not compromised.

Disclosure risk analysis is the examination or vetting by Statistics Canada employees of statistical output. This is done by analysing whether obvious identification of individual cases or whether information about individual cases can be inferred or deduced from the statistical output. There are three types of disclosures: identity; attribute; and residual.

Roles and Responsibilities

The audit revealed that the full-time RDC analyst at the University of Calgary performs this function for the Prairie Regional RDCs. He has knowledge and experience of statistical sampling techniques and software. Vetting is conducted using the survey-specific guidelines for 60 surveys on the RDC website. Questions or concerns with regards to the vetting process are addressed with the RDC regional manager on a weekly basis; at the RDC Annual meeting; and the RDC Confidentiality Committee whose mandate is to provide oversight to both the RDC analysts and the RDC program on disclosure risk analysis.

Researchers are provided training during their orientation session on the disclosure risk analysis process, various analytical methods and completion of the *"Disclosure Request Form"* for every output request.

Processes and Procedures

A detailed and comprehensive draft document *Disclosure Risk Analysis Guide for RDC Analysts* provides detailed step-by-step instructions with illustrations and flow-charts on how to conduct and perform disclosure risk analysis to the RDC analyst. Guidelines on disclosure risk analysis for various data types and descriptive or tabular output and variance-covariance and correlation matrices; graphs; models and example of *"Disclosure Request Form"* are also included.

An important part of the process is for researchers to complete the *"Disclosure Request Form"*, which requires them to list statistical sampling information. Should a "variable" not be understood by the RDC Analyst, the request is denied. It is the responsibility of the RDC Analyst to ensure that they understand what the variables mean, and their importance. Vetting guidelines are posted around the RDC facility and in electronic form on the workstations to ensure that researchers complete all the applicable sections in the form. Printing is directed to the network printer which is controlled by the RDC analyst. Coloured paper is used for files that have been vetted and allowed to be removed. This control allows analysts to visually detect what is being removed from the RDC facility.

The audit concluded that processes and procedures for disclosure risk analysis are in place and communicated to the RDCs by MAD HQ to reduce the risk of unwanted disclosure. A sample of randomly selected contracts was tested for disclosure risk analysis. This was done by reviewing the *"Disclosure Request Form"*; the related output files created; and the results of the disclosure risk analysis in the clearance request subdirectory created by the RDC analyst for discussion with the researcher for product creation and dissemination.

The audit determined that the RDC analyst ensures that Statistics Canada confidential data is not compromised by carefully administering and screening all requests for disclosure risk analysis.

Line of Enquiry #2: Research data centres comply with applicable Treasury Board of Canada Secretariat and Statistics Canada policies and standards regarding Information Technology Security and Physical Security to ensure that confidentiality of data is protected in the delivery of services at the regional research data centre.

Physical Security

Roles and responsibilities at both the program and the regional level are defined and communicated and authority is formally delegated at the program and operations level.

Physical security measures compliant with applicable TBS and Statistics Canada policies and standards are in place and adhered to for safeguarding and protecting Statistics Canada confidential data. Access to the Prairie Regional RDCs is restricted to authorized personnel, i.e. deemed employees, such as researchers and university IT support staff.

Physical security in RDCs should be compliant with applicable TBS policies, such as the Government Policy on Security and Statistics Canada's *Security Practices Manual*. Roles, responsibilities, and accountabilities should be defined, clear, and communicated. In the context of RDCs, physical security should include controls such as: physical access, intrusion detection and monitoring activities.

Roles and Responsibilities

The audit found that at the program level functional authority is formally delegated to the RDC Program Manager and at the regional level the RDC analyst and the statistical assistant are responsible for physical security. The RDC analyst reports to the RDC regional manager. The statistical assistant at Lethbridge reports to the University of Calgary full-time RDC analyst. The current financial agreement between Statistics Canada and the University of Calgary states that Statistics Canada is responsible for *"providing secure access to Statistics Canada data at the University, including physical security of the centre and electronic security of the data, security checks and access permissions"*. DS at HQ provides guidance and directives on physical security requirements. DS performs the physical and IT security inspections of the RDC sites and provides recommendations to the Manager. IT and physical security inspection of the University of Calgary RDC took place in April 2002 and of the University of Lethbridge RDC in October 2009 by DS before they became operational.

Assessment of the Physical Security Controls at the Prairie Regional Research Data Centres

To assess whether the Prairie Regional RDCs comply with TBS' *Government Policy on Security* and Statistics Canada's *Security Practices Manual*, a physical inspection of the Prairie Regional RDCs was carried out to test the physical security practices for operational accommodations outside the Statistics Canada complex at HQ.

Perimeter Security Controls

Both RDCs are located in the campus library building. The audit noted that both facilities are in compliance with TBS and Statistics Canada's requirements for perimeter security for 'shared floor occupancy' i.e. wall separation and construction; and solid-core wood doors with heavy-duty hardware and accessories.

Entry Security Controls

Physical access in and out of both the Prairie Regional RDCs is through a single entry point to allow for effective screening and monitoring by the RDC staff. Each single entry door is equipped with an electronic intrusion alarm and deadbolt lock for which only the RDC staff and campus security have the key. This is in compliance with TBS and Statistics Canada requirements.

Access Security Controls

To comply with TBS and Statistics Canada requirements, an electronic swipe card access system consisting of an identification card which contains electronic information identifying the owner is in place in both the RDCs to control access to the facility. The system registers all access into the RDC and RDC staff can request a print-out of the electronic card access register from campus security if required. Unauthorised visitors are not allowed past the single entry door of the RDC facilities.

Telecommunications Wiring and Restricted-Access Area Controls

The audit noted that IT related wiring is channelled through the walls and ceiling of both the RDCs. At the University of Calgary RDC there is a secure server room with locked storage cabinets for storing archived compact discs and researchers' files to protect confidential, classified, and protected information. Network B access is only available in a separate meeting room with a workstation. Since the University of Lethbridge RDC is new and significantly smaller, its server and network B access are secured in the statistical assistant's office. All workstations at both the RDCs have lockable cabinets and the keys are secured in the RDC analyst and statistical assistant's offices. This is in compliance with TBS and Statistics Canada requirements.

Cleaning and Maintenance Service Activities Controls

In compliance with TBS and Statistics Canada requirements, maintenance and cleaning personnel do not have access cards to the RDCs. Cleaning personnel can only access the RDC facilities during regular working hours and are escorted by the RDC staff. If access is required outside of normal hours of operations, cleaning and maintenance personnel are accompanied by campus security.

Intrusion Detection and Monitoring Activity Controls

Campus security provides 24/7 monitoring of the RDC facilities. They have an access card and security code to the alarm system. A camera surveillance system is installed in both the RDCs to enhance the security and is monitored by the full-time RDC analyst at the University of Calgary and by the statistical assistant at the University of Lethbridge.

RDCs cannot be left unattended; if the RDC analyst is required to leave the RDC for a period of time during regular hours, researchers are required to leave the RDC, the door is then locked and a sign is placed on the door.

Based on our physical inspection of the Prairie Regional RDCs, the audit determined that applicable physical security measures are in place and adhered to for safeguarding and protecting Statistics Canada confidential data and access to the Prairie Regional RDCs is restricted to authorized personnel, i.e. deemed employees, such as researchers and university IT support staff.

Information Technology Security

Roles and responsibilities at both the program and the regional level are defined and communicated.

Tests for access, identification and authentication safeguard measures on a randomly selected sample of contracts revealed that they are in place and working as intended.

Assessment of the system and communications protection safeguards revealed that opportunities exist to strengthen the computing environment by ensuring that all USB ports on all stand-alone workstations are disabled and by reducing the login timeout of the workstations.

Information technology security in RDCs should be compliant with applicable TBS policies, such as the *Operational Security Standards: Management of IT Security* and Statistics Canada's *Security Practices Manual.* Roles, responsibilities, and accountabilities should be defined, clear, and communicated. In the context of RDCs, IT security should include System and communications protection: security controls that support the protection of the information system itself as well as communications with and within the information system; Access control: security controls that support the ability to permit or deny user access to resources within an information system; and Identification and authentication: security controls that support the unique identification of users and the authentication of these users when attempting to access the information system.

Roles and Responsibilities

The audit noted that the accountability structure for IT security in the Prairie Regional RDCs is the same as that for physical security.

System and Communications Protection Safeguards

The computing environment inside the RDCs consists of stand-alone workstations for use by the researchers. They are not connected to the internet. Internet access is only available to the RDC employees and in the workstation located in the meeting room at the University of Calgary RDC. The workstations run the standard Statistics Canada operating system and desktop software configuration and approved statistical software such as SPSS, Stata, or SAS. The audit noted that specific software requested by the researchers is installed by the RDC analyst, after receiving approval from the Information Technology Services Division at HQ. This is allowed by the RDC program.

At the University of Calgary RDC, the USB ports on 11 of the 14 workstations were enabled; significantly increasing the risk of undetected removal of Statistics Canada confidential microdata using a USB key. The audit determined that there has been no reported security breaches or incidents recorded for the unauthorized removal of confidential microdata at the RDC. Login timeouts were found to be either set to 45 minutes or did not function consistently; increasing the risk of allowing unauthorized access to Statistics Canada confidential microdata on unattended workstations.

There is a fax machine located in the University of Calgary RDC meeting room available for researchers which increases the risk of undetected or unauthorized transmittal of Statistics Canada confidential information by researchers.

Access, Identification and Authentication Safeguards

A sample of randomly selected contracts which included 26 of 182 contracts (14%) as of December 2010, for the Prairie Regional RDCs were tested for access, identification and authentication controls. This was done by reviewing the folder contents in the sample against their master file to ensure that all filenames were part of the original datasets; reviewing the event logs for deleted user IDs in the sample to ensure that they had no access; and reviewing the active directory for user names and dataset permission to ensure that they existed for only active contracts in our sample.

The audit tests revealed that access to systems, microdata files and programs is restricted to researchers with active contracts. 7 of the recently completed contracts were verified in the event log to ensure that there had been no access to the associated microdata files since their completion date. Results revealed that no access has occurred. The audit noted that microdata files are not removed from the server after all associated contracts using those files have terminated. This practice is supported by the RDC program to allow the RDCs to maintain a local library of all the files accessed at the respective RDC.

Procedures specify that user accounts should be created only when a contract is approved and becomes active; access should be removed if the account is not active. Creation of user accounts and the granting of access to microdata files were substantiated by approved active contracts in all sampled contracts. Passwords meet Statistics Canada standards but remain the same for the duration of the contract which can range anywhere from one year to several years. Statistics Canada's *Security Practices Manual* requires maximum password life be set to 90 days.

Administrative privileges rest with the RDC analyst. As such, the RDC analyst is responsible for creating a folder for each approved project and creating an associated user account and password for each researcher for read-only access to the folder. Therefore, researchers are not able to: access microdata files for which they do not have an approved project; view contents of data sets not specified in their proposal; and move files (documents, datasets, syntax or output) from one research project to another. Once a user account is created, the RDC analyst notifies the university campus security to issue a faculty/student identification card that provides access to the RDC facility.

The audit determined that applicable IT security measures are in place and adhered to for safeguarding and protecting Statistics Canada confidential data. IT access, identification and authentication safeguard measures are in place at the RDCs and are working as intended.

Recommendations:

It is recommended that the Assistant Chief Statistician Social, Health and Labour Statistics Field ensure that:

- *Passwords and login timeout mirror Statistics Canada's Security Practices Manual*
- *Workstation USB ports are disabled*
- *The fax machine is moved out of the researchers' meeting room in the University of Calgary RDC.*

Management Response:

Management agrees with all of the recommendations.

- The Manager, MAD has referred the password and login timeout standards to the RDC Technology Committee to incorporate in the centralized authentication process that is currently being set up.

  Deliverable and Timeline: Centralized authentication prototype by March 31, 2012 and migration of RDCs through 2012/2013.
- The Manager, MAD has ensured that all USB ports have been re-disabled and a monthly checklist for analysts to verify ongoing security practices has been prepared by the Technology Committee.

  Deliverable and Timeline: Monthly check-list. Completed.
- The Manager, MAD has ensured that the fax machine has been moved into the analyst's office.

  Deliverable and Timeline: Completed.

Appendix

Appendix A: Audit Criteria

Line of Enquiry/Core Controls	Criteria
1) Research Data Centres have effective practices and mechanisms in place to ensure that the confidentiality of data is protected in the delivery of services at the regional Research Data Centre.	
Accountability	1) Responsibilities are formally defined and communicated. 2) Authority is formally delegated and aligned with individual's responsibilities and incompatible functions are not combined.
Risk Management	1) Risks are identified and take into consideration internal and external environments of the RDC program. 2) Formal processes and guidelines exist to assess controls and manage identified risks.
Public Service Values	1) Employees acknowledge compliance with Statistics Canada's corporate values and ethics and code of conduct.
Results and Performance	1) Responsibility for monitoring is clear and communicated and results are reported to required authority levels. 2) Active monitoring is demonstrated.
2) Research Data Centres comply with applicable Treasury Board of Canada Secretariat and Statistics Canada policies and standards regarding Information Technology Security and Physical Security to ensure that confidentiality of data is protected in the delivery of services at the regional Research Data Centre.	
Accountability	1) Functional authority for IT and physical security as it relates to the RDC program is appropriately vested in and exercised by functional heads. 2) The organization structure permits clear and effective lines of communication and reporting.
Risk Management	1) IT and physical security control assessments exist with input from relevant corporate service functions.
Stewardship	IT Security: 1) Processes, procedures and controls for safeguarding Statistics Canada microdot files include: ➢ *logical access controls* – to control access to microdata files according to the terms of the Microdata Research Contracts (MRCs) ➢ *computer systems security* – to help ensure electronic protection of the data and prevent and detect security

Stewardship (continued)	vulnerabilities. 2) Authentication and access procedures and mechanisms exist. 3) IT controls include a mix of automated and manual controls and their operating effectiveness is periodically tested. 4) The processes governing access to data adhere to applicable TBS and Statistics Canada IT security policies and exceptions are identified and appropriate actions are taken. Physical Security: 1) Physical security measures adhere to applicable TBS and Statistics Canada policies and procedures. 2) Access to the RDC facility is physically restricted and enforced for the protection of sensitive assets and procedures to safeguard and protect the use of assets exist and are adhered to.