Statistics Canada Statistique Canada

Final Audit Report

Audit of Data-Sharing Agreements

April 15, 2010

Project Number: 80590-60

Canada

Table of Contents

Executive Summary

Data-sharing agreements (DSAs) under sections 11 and 12 of the *Statistics Act* have been practiced by Statistics Canada since 1976. DSAs have become a key business process. These agreements now number 500, cover nearly all of the business surveys and a majority of household surveys, and enjoy certain exceptions regarding the release of confidential respondent information. In recent years, data-sharing have become a growing and increasingly complex area to manage. Ensuring confidentiality protection of shared data, a key value of Citizen-Focused Service, Public Service Values and Stewardship at Statistics Canada, is a challenge. DSAs are covered by a multi-party management framework, characterized by a distributed management under various responsibility arrangements between the units of Statistics Canada and DSA partners (external Canadian organizations). The risks of non-compliance to the legislative and policy requirements on confidentiality protection and the damage to reputation of Statistics Canada were ranked as high.

The objectives of this audit were to provide the Chief Statistician and the Departmental Audit Committee (DAC) with assurance that Statistics Canada's DSA Confidentiality Management Control Framework (MCF) is adequate and effective over the entire life-cycle of DSAs; and activities supporting the DSA Confidentiality MCF are compliant with the Government of Canada and Statistics Canada acts and policies on confidentiality over the entire life-cycle of DSAs.

The audit was conducted by the Internal Audit Services of Statistics Canada and the evidence was gathered in compliance with the Internal Audit Standards for the Government of Canada and the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors.

The audit found that Statistics Canada and its partners are compliant with the relevant acts and policies. However, opportunities exist to strengthen the management control framework related to DSAs in the areas of risk management, monitoring and information management and communication.

DSA Confidentiality Management Control Framework is composed of 5 elements: planning and reporting, information management and communication, risk assessment, monitoring and the confidentiality compliance environment. DSA confidentiality compliance environment as an element of the management control framework is satisfactory. The audit determined that there is no single comprehensive document or policy on the management of DSAs that would combine all relevant confidentiality compliance requirements, covering the entire DSA life-cycle and establishing an appropriate management control framework.

Systematic risk management is an underpinning of good government. The DSA management control framework has fragmented and often ad-hoc practices related to risk

management when assessing confidentiality compliance. Opportunities to advance the risk management practices exist at the departmental and divisional level.

Access to information is a key value of Statistics Canada, which includes access to shared data by DSA partners under the data-sharing agreements. The audit found dormant DSAs and instances when shared data were not being provided to partners in a timely manner. Information management and communication practices would benefit from the improved integration of records and development of integrated protocols.

With respect to the DSA confidentiality compliance status, Statistics Canada and DSA partners are compliant with the legislative and policy requirements, no confidentiality breaches have been detected. However, the information required to assess confidentiality compliance was often fragmented and incomplete at the monitoring stage of the DSA life-cycle. A management monitoring regime would provide sufficient and reliable information for decision-making as it relates to relevance and confidentiality management.

Overall, there is an opportunity to advance to a strategic model of risk management and apply the principles of active monitoring with regards to DSAs, which would improve management effectiveness.

Introduction

Background

For more than 30 years Statistics Canada had exercised its mandate to enter into statistical data-sharing agreements (DSAs) with other organizations under the authority of sections 11 and 12 of the *Statistics Act.* DSAs have become a key business process. These agreements now number 500, cover nearly all of the business surveys and a majority of household surveys, and enjoy certain exceptions regarding the release of confidential respondent information either with or without the respondent consent, provided that the legal requirements for the provision of data-sharing information, consent rights and confidentiality protection are respected by all parties. In general, data-sharing for statistical purposes occurs when statistical and information inquiry is initiated by joint survey partners, or where a common data resource is equally and jointly owned by two or more partners. Data-sharing is exercised when there are significant reductions in response burden and compliance costs for data-sharing partners, as well as improvements in statistical data accuracy, coverage, relevance and timeliness.

Specifically, the *Statistics Act* allows for two types of DSAs[1]:

- s.11 DSAs: data-sharing with provincial/territorial statistical offices that are subject to legislation similar to the federal *Statistics Act*, which provides the authority to collect information for statistical purposes and to compel response from respondents and to request mandatory data-sharing; it stipulates legal requirements to ensure confidentiality protection of the respondent information and to notify respondents of the planned data-sharing;
- s.12 DSAs: data-sharing with other federal government departments, non-statistical provincial government departments, municipal corporations and other legal entities, which either have (according to their own legislation) or do not have the legal authority to compel response and to request mandatory versus voluntary data-sharing; it stipulates legal requirements to ensure confidentiality protection of the respondent information, to notify respondents of the planned data-sharing, and, in case of the voluntary data-sharing, to inform respondents about their right to object to data-sharing.

In 2008, the volume of statistical data-sharing agreements has reached the 500 mark. Most of the DSAs, or 94% of them, are classified as providing for voluntary data-sharing. These fall under s.12 DSAs, where respondents have the right to refuse to share the information. The rest of the agreements are split between the mandatory data-sharing under s.11 provincial/territorial DSAs (4%) and mandatory data-sharing under so-called

[1] "Data-sharing between Statistics Canada and other organizations: A primer", http://www44.statcan.ca/2008/11/s0400-eng.htm.

s.12+ DSAs (2%)[2]. The accumulation of DSAs is a reflection of the need for cooperation between Canadian organizations in the collection, compilation and publication of the statistical information.

At the same time, the federal privacy and security control environment has tightened and became more complex when the *Privacy Act* (1985), TBS Policy on Privacy Impact Assessment (2002) and Government Security Policy (2002) came into effect. In response, Statistics Canada has established broad control mechanisms[3] for the confidentiality protection of the respondent data, including those obtained under the DSAs.

The DSA Confidentiality Management Control Framework (DSA Confidentiality MCF) is defined as a way in which Statistics Canada and DSA partners organize themselves in order to distribute, coordinate, and manage confidentiality risks associated with the data-sharing processes and to ensure compliance with the relevant acts and policies. There are three major groups of legislative and policy requirements for DSAs that confidentiality management control framework covers: 1) the general DSA information (ISR) and consent rights management; 2) the general DSA confidentiality protection management (i.e. physical, IT and personnel security); and 3) the DSA-specific confidentiality safeguards (in this case, third-party data-sharing or sharing with other parties).

DSA Confidentiality MCF for Statistics Canada is characterized by a distributed management, with separate mandates and various responsibility arrangements among the following key parties**:**

- STC departmental unit**:** Data Access and Control Services Division (DACS) in the consulting and legal verification role;
- STC divisions**:** survey-managing divisions that are responsible for the implementation and operations of associated DSAs (this includes oversight of collection areas and collection partners);
- DSA partners**:** federal, provincial/territorial or municipal governments and other Canadian legal entities.

Objectives

The objectives of this audit were to provide the Chief Statistician and the Departmental Audit Committee (DAC) with assurance that:

1. Statistics Canada's DSA Confidentiality MCF is adequate and effective over the entire life-cycle of DSAs.
2. Activities supporting the DSA Confidentiality MCF are compliant with the Government of Canada and Statistics Canada acts and policies on confidentiality over the entire life-cycle of DSAs.

[2] s.12+ refers to the amendment of s.12 of Statistics Act, which authorizes mandatory data sharing with other federal or provincial government departments and organizations who have the legal authority to compel response in addition to Statistics Canada's, and who use the data in accordance with their own governing legislation.
[3] Policy on Informing Survey Respondents and associated guidelines, Privacy Impact Assessment Policy and associated guidelines, Policy on Security of Sensitive Statistical Information and associated guidelines, IT Security Policy and associated guidelines, etc.

Scope and Approach

The audit engagement was conducted in conformity with the Internal Audit Standards for the Government of Canada and the International Professional Practices Framework (IPPF) of the Institute of Internal Auditors. All work was conducted in collaboration with DACS, Statistics Canada's divisions and DSA partner managers responsible for the DSAs selected in the audit sample. The audit approach was inspired by the Government of Canada Management Accountability Framework (MAF) and the Core Management Control Guidelines issued by the Office of the Comptroller General (audit criteria, Appendix A).

The audit universe consisted of 500 active and formalized DSAs, pertaining to s.11, s.12 and s.12 + DSAs for the period of 1976-2008 (see Appendix B). The scope of the audit included:

- the assessment of Statistics Canada multi-party DSA Confidentiality Management Control Framework established for a system of DSAs, covering the period of October 1976 to October 2008 and all DSAs; and
- the conduct of tests of compliance controls for the selected active formalized DSAs: a sample of 39 DSAs, of which 31 agreements were s.12 DSAs (for the period of October 2006-08) and 8 s.12+ DSAs (all of them); the sample covered 80 business and social surveys, 10 DSA managing divisions at Statistics Canada and 32 DSA partners.[4]

Assessing the DSA confidentiality management control framework involved comprehensive examination of multi-party DSA confidentiality compliance practices along such dimensions as DSA confidentiality compliance environment, risk assessment, planning and reporting, information and communication, and monitoring with respect to the three groups of legislative and policy requirements (see Appendix C). To perform the audit work, the following methods were used: audit interviews with Statistics Canada management, audit surveys, examinations of controls and compliance tests.

Excluded from the scope of tests of compliance controls were s.12 DSAs formalized prior to October 2006 due to significant management changes, i.e. introduction of enhanced confidentiality controls and review and audit clauses by Statistics Canada; and all s.11 DSAs due to their relatively lower risk level[5].

Authority

The audit was undertaken by the Internal Audit Services in accordance with the Statistics Canada's Risk-Based Audit Plan for the fiscal years of 2008/09-2010/11 which was approved by the Internal Audit Committee on March 19th, 2008.

[4] Sample adequately represents a range of federal government departments, provincial non-statistical government agencies and other organizations, and miscellaneous legal entities in Canada (including aboriginal organizations).

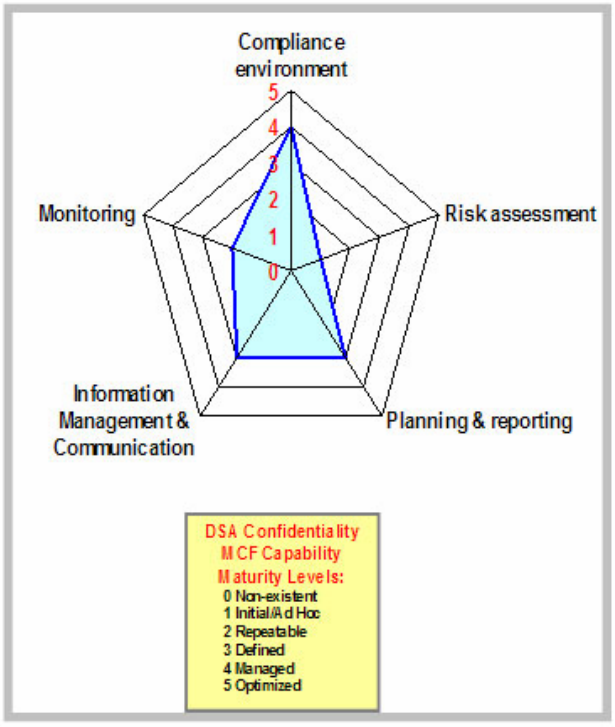
[5] In addition, enhanced confidentiality protection compliance inspections of the provincial/territorial statistical focal points have been consistently conducted by Statistics Canada during the period of 2001-2008 for the purposes of CRA MOU.

Findings, Recommendations and Management Responses

An adequate and effective management control framework for DSA confidentiality compliance, in relation to three groups of legislative and policy requirements, would include planning and reporting, information management and communication, risk assessment, monitoring and compliance environment.

In relation to objective 1, out of the five MCF dimensions, only the DSA confidentiality compliance environment is fully managed (see Figure 1). The rest of the MCF elements are at various stages of development, with particular weaknesses in risk assessment, information management and communication, and monitoring, requiring a range of improvements.

Figure 1. DSA Confidentiality MCF Assessment Snapshot



DSA confidentiality compliance environment as an element of the MCF is satisfactory. However, the audit determined that there is no single comprehensive document or policy on the management of DSAs that would combine all relevant confidentiality compliance requirements, covering the entire DSA life-cycle and establishing an appropriate MCF.

Systematic risk management is an underpinning of good government. The DSA management control framework has fragmented and often ad-hoc practices related to risk management when assessing confidentiality compliance.

Access to information is a key value of Statistics Canada, which includes access to shared data by DSA partners under the data-sharing agreements. The audit found dormant DSAs and instances when shared data were not being provided to partners in a timely manner. Information management and communication practices would benefit from improved integration of the records and development of integrated and standardized protocols.

In relation to objective 2, Statistics Canada and DSA partners are compliant with the legislative and policy requirements on confidentiality protection; however, the information required to assess compliance was often fragmented and incomplete at the monitoring stage of the DSA life-cycle.

All recommendations and management response and action plans (MRAPs) should be considered within the existing Statistics Canada management structure.

DSA Confidentiality Compliance Environment

DSA confidentiality compliance environment element of the MCF is satisfactory, and is characterized by a distributed management between Statistics Canada and DSA partners. There is no single document or policy on the management of DSAs that would combine all relevant confidentiality compliance requirements and establish a strong management control framework covering the entire DSA life-cycle for all parties involved.

Adequate and effective management of DSAs would include confidentiality compliance controls, governance structures, accountability and responsibility mechanisms, training and operational processes over their entire life-cycle. The audit identified that DSA confidentiality compliance environment is defined, communicated and managed between DSA parties, especially at the design and negotiation stage of the agreements. However, the environment is complex and difficult to navigate, and characterized by an absence of an integrated policy framework to manage DSAs.

DSA confidentiality compliance requirements are defined by the means of preventative controls found in the Statistics Act, Privacy Act, STC Policy on Privacy Impact Assessments (PIA), STC Policy on Informing Survey Respondents (ISR), STC Policy on Security of Sensitive Statistical Information, STC IT Security Policy, STC Policy on Micro-Data Release, STC Policy on Discretionary Disclosure and associated guidelines. Provisions for DSAs in legislative and policy references are quite fragmented and difficult to piece together for those who are not dealing with them on the daily basis. Specific standards for the confidentiality compliance are defined by the texts of DSAs and associated security appendices. This is further complicated by the fact that DSAs often combine multiple requirements from various jurisdictions which are subject to change, often making standardization difficult.

Strategic DSA governance and oversight framework is established and coordinated among DSA parties. Statistics Canada has a Confidentiality and Legislation Committee[6] that accommodates hearings for DSA concerns and proposals from divisions, DACS and DSA partners resulting in decisions and action plans. Other internal management committees, such as the Policy Committee, also get involved when necessary. DSA partners can be significantly involved during the implementation stages of DSAs via the Steering and Advisory Committees or Technical Groups associated with surveys that are covered by DSAs. This process allows all parties to exchange information about the DSA confidentiality compliance issues.

The operational authorities and responsibilities for DSA confidentiality compliance are distributed among the multiple parties. These responsibilities are limited by the mandates of these parties and are not necessarily carried through the entire life-cycle of a DSA. The departmental function of Data Access and Control Services is dedicated to the legal and

[6] Confidentiality and Legislation Committee reports to Policy Committee.

policy review, negotiation and approval of DSAs, their modification and termination, as well as coordination of associated requests in between these stages from either subject-matter divisions or DSA partners. DACS has a limited mandate to ensure accountability for DSA confidentiality compliance during implementation and monitoring stages, aside from provision of services to both divisions and DSA partners. Survey and DSA managing divisions consult with DACS during the planning stage and the implementation of DSAs using a set of internal support partners in the fields of collection services, communications, IT, or joint collection with external DSA partners. The joint management of DSAs between two or more Statistics Canada divisions is also practiced depending on the complexity of the DSAs, for which there are no clear guidelines on the roles and responsibilities. DSA partners are responsible for ensuring compliance with the terms of the DSAs during the implementation stages of the agreements.

It was found that DSA confidentiality compliance control processes are incorporated into much larger control mechanisms of survey operations. Compliance of DSAs with general information and consent rights requirements is embedded into the Survey Prescription processes. General confidentiality protection requirements for DSAs are incorporated into generic requirements on the physical, IT and personnel security, for which security checklists and procedures exist. DSA-specific safeguards, such as prohibition of third-party data-sharing or allowance for restricted access for researchers and research organizations of DSA partners under certain conditions, are specified in the agreements. Thus, managers have to combine all of these fragments into their own rules and processes, resulting in rather diverse practices for DSA confidentiality compliance management at the divisional level. Further, 90% of the divisions do not have dedicated managers for DSAs. Rather, responsibility for operational DSA management falls on the shoulders of survey managers. 80% of divisions do not have written manager's guides. There are no integrated operational protocols or manuals dedicated to DSAs in all 5 dimensions of MCF.

To mitigate the complexity of this environment and to ensure compliance, DACS provides extensive training programs in all generic areas related to confidentiality. This training covers the basics of legislative and policy compliance requirements, with some references to DSAs. However, it is not specific and operational enough for managers to be fully confident in its application. This results in DACS being overwhelmed by the constant requests for advice, clarifications, reviews, formal letters, custom training sessions, etc.

The absence of an integrated DSA management policy or framework adds to the complexity of the task of managing DSA confidentiality compliance and increases the risk of misinterpretation and confusion, potentially resulting in breaches of confidentiality. This may also result in heterogeneous and erroneous applications of DSA confidentiality compliance requirements. Having one integrated policy will provide greater overall clarity for the DSA confidentiality compliance environment.

Recommendation No. 1

It is recommended that Assistant Chief Statistician Corporate Services ensure that Data Access and Control Services develop a comprehensive and integrated Policy on the Management of Data-Sharing Agreements to provide adequate control coverage over the entire DSA life-cycle.

Management Response

Management accepts the recommendation.

DACS will develop a DSA governance process guided by a policy or directive, which will be integrated with the risk management framework. In addition, divisions will be asked to report on this element as part of the new Statistics Canada Quadrennial Program Review (QPR) guidelines.

Deliverables and timelines:
Presentation of the governance process to the Confidentiality and Legislation Committee.
Integration of this element into the Quadrennial Program Review (QPR) guidelines.
Director, Data Access and Control Services and Director, Corporate Planning and Evaluation Division – October 2010

DSA Risk Assessment

DSA risk management practices are in the early development stage and its risk assessment is fragmented, ad-hoc and managed informally.

An appropriate risk management model would include adequate and effective practices for assessment of the risks of non-compliance and/or non-reporting for breaches and weaknesses related to DSA confidentiality. The audit revealed that systematic and formal mechanisms for the DSA risk assessment are not in place, but are rather fragmented, ad-hoc and managed informally.

At the departmental level (DACS), it was found that the risks of non-compliance for the general DSA information and consent rights management are assessed at the DSA design & negotiation stage by generic or specific Privacy Impact Assessments. The risks of non-compliance for the other two groups of requirements, i.e. general DSA confidentiality protection and DSA-specific confidentiality safeguards are not formally assessed by DACS due to the newness of the risk management initiative at Statistics Canada. At the divisional level, due to limitations in the mandate of DSA-managing divisions, half of the directors assessed their DSA risk assessment processes as managed informally and unsystematically, while the other half admitted that there is no activity in this area. However, all confirmed that the procedures for reporting on the breaches and weaknesses

of the confidentiality controls are known and implemented when breaches are reported. It is expected that employees making mistakes will come forward or will be detected. At the DSA-partners level, the evidence is not sufficient to provide a conclusion.

There is a risk that the lack of formal, integrated and continuous risk management practices for DSA confidentiality and non-reporting risks across all DSA parties will not detect confidentiality breaches and may prevent adequate and effective risk mitigation strategies.

An innovative practice exists in Health Statistics Division, which controls the risks that respondent non-sharers can be mistakenly identified as sharers during the collection period by monitoring the collection processes for various surveys. It also maintains a spreadsheet file to identify risks related to DSAs.

Recommendation No. 2

It is recommended that Assistant Chief Statistician Corporate Services ensure that Data Access and Control Services, in consultation with Corporate Planning and Evaluation, strengthen the risk management practices with respect to DSAs.

Management Response

Management accepts the recommendation.
DACS will conduct a threat and risk assessment with respect to the management of DSAs. This will result in a report outlining the potential threats, and the steps that could be taken to eliminate or reduce the risks.
The process will be repeated regularly.
The report will be presented to the Confidentiality and Legislation Committee.

Deliverables and timelines:
Presentation of the report to the Confidentiality and Legislation Committee.
Director, Data Access and Control Services and Director, Corporate Planning and Evaluation Division – October 2010

DSA Information Management and Communication

DSA information management and communication practices as an element of MCF are defined, but would benefit from further integration and modernization.

An appropriate information management and communication model would include adequate and effective systems, processes and protocols to form comprehensive DSA records and to gather relevant statistics on DSA confidentiality compliance performance to facilitate the senior management decision-making process. Data-sharing is exercised

when there are significant reductions in response burden and compliance costs for data-sharing partners, as well as improvements in statistical data accuracy, coverage, relevance and timeliness. The audit identified that DSA information management and communication systems and processes are disconnected between DACS and DSA-managing divisions, and are managed according to their mandates. This practice results in heterogeneous records and gaps in information and communication coverage during the DSA life-cycle. Knowledge management systems and processes are predominantly informal.

At the departmental level, it was found that information is spread over several media: paper files, DACS Administrative Database, and server files. Combined, these sources provide information for decision making, but require integration. Indicators found in the DSA database are useful, but are applicable mostly during the beginning and end of the DSA life-cycle, when DACS controls legal processes. However, rather limited information is available in the middle of the DSA life-cycle. There are no provisions in the systems and processes for the collection and analysis of information on DSA confidentiality compliance.

At the divisional level, the audit revealed that DSA managing divisions structure their own operational information and communication processes. It was found that they have not established systematic and integrated information management, communication and record systems and processes, but rather have what they consider as essential records to reflect their transactions with DSA partners, providing incomplete information. Divisional managers over-rely on DACS for information, believing they can always have access to DSA legal files and documentation on request. 60% of the directors see the need for a central DSA electronic database to enable pro-active management and monitoring of the DSAs.

The audit identified that there is a communication issue between DSA parties regarding the timing of the release of the shared data. DSA-managing divisions make an assumption that DSA partners will request the shared data file upon announcement of the release in the external flagship publication of Statistics Canada, the “Daily”. However, this was not the case. Additionally, the majority of the DSA partners had difficulty providing information in a timely manner during the audit procedures.

There is a risk that a sub-optimal DSA information management and communication model will not provide a timely, accurate, continuous and holistic “big picture” of DSAs to aid an effective decision-making process.

Recommendation No. 3

It is recommended that Assistant Chief Statistician Corporate Services ensure that Data Access and Control Services strengthen the information management and communication practices for DSAs.

Management Response

Management accepts the recommendation.
DACS will develop a departmental directive to formally describe the required practices. The draft directive will be presented to the Confidentiality and Legislation Committee.

Deliverable and timeline:
Presentation of the draft directive to the Confidentiality and Legislation Committee.
Director, Data Access and Control Services – October 2010

DSA Confidentiality Compliance Status

Statistics Canada and DSA partners are compliant with the legislative and policy requirements on confidentiality protection, but implementing a strong management monitoring regime would facilitate the management of all DSAs.

We expected to find compliance with the Government and Statistics Canada policy framework, the legislative requirements and the terms and conditions of the DSAs over their entire life-cycle. The audit identified that Statistics Canada and DSA partners are compliant with the legislative and policy requirements, but the information, which would normally be acquired through a monitoring program, is insufficient.

In 2006, DACS started to gradually introduce a review and audit clause into the texts of the DSAs, where the partners would agree to it. However, the capacity to exercise the clause on a systematic basis does not exist. The onus is on Statistics Canada DSA-managing divisions and DACS to verify that partners follow the rules. DSA confidentiality compliance monitoring, defined as practices encompassing evaluations of DSA confidentiality compliance controls, reporting and exchanging information on control weaknesses and their correction, as well as change management, is not envisaged by the current legislative and policy suite. A few years ago, DACS asked the s.11 DSA partners to conduct a self-assessment and submit their reports.

With respect to compliance with general DSA information and consent rights requirements**,** the audit identified that at the departmental level, the ISR and PIA processes for the verification of survey materials and DSA texts are well managed. At the divisional level, the audit indicated that improvement is required regarding monitoring of the DSA ISR and consent rights requirements during the survey implementation and collection of compliance performance information from the collection areas. A mechanism to collect respondent objections/waivers to data-sharing is in place for all of the divisions in the audit sample. However, only half of them stated that they have a documented procedure for processing these data, collecting reports from collection areas and using this information further in the preparation of shared files.

The audit found that requirements on general DSA physical, personnel, IT security and disclosure management are adequately specified in the texts of the agreements, and compliance by Statistics Canada staff and DSA partners is observed. The audit revealed that 34% of DSA partners reported that they have not established any processes yet, because they have not requested the data or that they are not planning to request the data.

With respect to compliance with DSA confidentiality safeguards regarding conditions for data-sharing with other parties, the audit found that prohibition of third-party data-sharing is specified in the texts of DSAs or clarified during the negotiations process. In exceptional circumstances, third-party data-sharing is allowed on the basis of legislative and security review by DACS. In the "Uses of Information" clause of the agreements, the research contractors and research organizations working directly for the DSA partners can be allowed access to shared data under very strict security and non-disclosure conditions. The audit identified that often research contractors and research organizations are engaged by the DSA partners once the shared data become available well into the implementation or monitoring stages of the DSAs. Regardless of the voluntary or mandatory nature of the DSAs, divisions have rather limited processes for coordination and monitoring of data-sharing with other parties. Managers know the provisions of the DSAs, however, systematic documentation regarding how these processes are managed was not available in all instances during the audit.

Monitoring practices are not systematic, have limited coverage and do not provide complete DSA information as it relates to confidentiality. The risk of insufficient monitoring may result in the failure to detect weaknesses and confidentiality breaches in relation to the DSA legislative and policy requirements. Consequently, timely and effective corrective measures cannot be implemented. The lack of a strong monitoring regime results in an accumulation of dormant DSAs, which would ideally be terminated or modified.

An innovative practice has been identified in Business Special Surveys and Technology Statistics Division (BSSTSD). A system is in place to track and monitor waivers for data-sharing. The written waivers are noted in the data-capture system (PC-BOSS) and the letters are stored in locked cabinets for reference. Information on the waivers is monitored through this system and queries are used to eliminate respondents who objected to data-sharing with specific partners. In addition, interviewers are physically monitored during collection process to ensure compliance to policy requirements on data-sharing.

Recommendation No. 4

It is recommended that the Assistant Chief Statistician Corporate Services ensure that Data Access and Control Services implement a DSA monitoring program.

Management Response

Management accepts the recommendation.

DACS will develop a proposal for a DSA monitoring program, including resource requirements. In addition to employee time to manage the monitoring, travel costs will be required.
The proposed monitoring program will be presented to the Confidentiality and Legislation Committee.

Deliverable and timeline:
Presentation of the monitoring plan to the Confidentiality and Legislation Committee.
Director, Data Access and Control Services – October 2010

Appendices

Appendix A: Audit Criteria

1.1. DSA multi-party confidentiality compliance environment is adequate and effective and satisfies MAF Citizen-Focused Service CFS-1, CFS-3, CFS-4 and Stewardship ST-22 criteria

1.2. DSA multi-party confidentiality compliance risk assessment practices are adequate and effective and satisfy MAF Citizen-Focused Service CFS-1, CFS-3, CFS-4 and Stewardship ST-22 criteria

1.3. DSA multi-party confidentiality compliance control planning & reporting practices are adequate and effective and satisfy MAF Citizen-Focused Service CFS-1, CFS-3, CFS-4 and Stewardship ST-22 criteria

1.4. DSA multi-party confidentiality compliance information & communications practices are adequate and effective and satisfy MAF Citizen-Focused Service CFS-1, CFS-3, CFS-4 and Stewardship ST-22 criteria

1.5. DSA multi-party confidentiality compliance monitoring practices are adequate and effective and satisfy MAF Citizen-Focused Service CFS-1, CFS-3, CFS-4 and Stewardship ST-22 criteria

2.1. General DSA information and consent rights management by all DSA parties over its life-cycle is compliant with relevant acts and policies and associated guidelines, MAF Public Service Values PSV 1-4 and Stewardship ST-22 criteria

2.2. General confidentiality protection management by all DSA parties over its life-cycle is compliant with Statistics Act, GoC Security Policy, StatCan's Policy on Security of Sensitive Statistical Information, IT Security Policy and associated guidelines, MAF Public Service Values PSV 1-4 and Stewardship ST-22

2.3. Management of DSA-specific confidentiality safeguards by all DSA parties over its life-cycle is conducted according to the terms of the agreement and MAF Public Service Values PSV 1-4 and Stewardship ST-22

Appendix B: Cumulative Number of Active Formalized Statistics Canada Data-Sharing Agreements at the end of 2008

Jurisdiction - Juridiction	Section - Article		
	11	**12**	**12+**
Federal - Fédéral	0	113	6
Newfoundland - Terre-Neuve	2	23	0
Prince Edward Island - île-du-Prince-Édouard	0	25	0
Nova Scotia - Nouvelle-Écosse	1	23	0
New Brunswick - Nouveau-Brunswick	1	23	0
Quebec - Québec	5	30	0
Ontario - Ontario	1	27	0
Manitoba - Manitoba	7	29	0
Saskatchewan - Saskatchewan	1	23	2
Alberta - Alberta	1	30	2
British Columbia - Colombie-Britannique	1	28	0
Yukon - Territoire du Yukon	1	13	0
Northwest Territories - Territoires du Nord-ouest	0	13	0
Nunavut - Nunavut	0	4	0
Miscellaneous - Divers	0	65	0
Total	**21**	**469**	**10**

Appendix C: Glossary

DSA Confidentiality Management Control Framework (MCF) - A way in which Statistics Canada and DSA partners organize themselves in order to distribute, coordinate, and manage confidentiality risks associated with the data-sharing processes and to ensure compliance with the relevant acts and policies.

DSA Confidentiality MCF Architecture includes:

1st tier: Confidentiality compliance requirement groups
- general DSA information and consent rights management
- general DSA confidentiality protection management
- DSA-specific confidentiality safeguards

2nd tier: Compliance framework
- DSA multi-party confidentiality compliance environment;
- DSA multi-party confidentiality compliance risk assessment practices;
- DSA multi-party confidentiality compliance control planning & reporting practices;
- DSA multi-party confidentiality compliance information & communications practices;
- DSA multi-party confidentiality compliance monitoring, change management and corrective practices.

3rd tier: Corporate Control Framework groups
- Acts, policies, guidelines, standards
- Accountability & responsibility centres
- Systems & processes

4th tier: DSA life-cycle stages
- Design & negotiation
- Implementation
- Monitoring
- Modification/termination

DSA Life-Cycle - Period from the start to the end of activities for the DSA project; divided into the 4 stages:
1. **DSA design & negotiation** – the period from the start of communications between the DSA partners on the potential DSA project and the signing of the agreement.
2. **DSA implementation** – conduct of the data collection and data transmission activities.
3. **DSA monitoring** – monitoring of the compliance of the DSA partners to the terms of the agreement; monitoring of changes in the conditions, etc. It also means conduct of communications with the parties involved in the Management Control Framework, evaluations, inspections, assessments, reviews of the various controls, etc.
4. **DSA modification/termination** – the period from the start of communications between DSA partners on the changes to the status of the agreement until it is revised or terminated.

Management Control - Any action taken by management and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

ISR – Informing Survey Respondents, Statistics Canada policy and associated processes and mechanisms.

PIA – Privacy Impact Assessment, Statistics Canada policy and associated processes and mechanisms.