Employment and
Social Development Canada

Emploi et
Développement social Canada

Unclassified

Internal Audit Services Branch

Audit of the Management and Delivery of the Social Insurance Number Program

December 2015

Canada

Table of Contents

Executive Summary

The Social Insurance Number (SIN) is a unique file identifier used for a variety of Government of Canada benefits and services. The SIN is the responsibility of Employment and Social Development Canada (ESDC) as legislated by the *Department of Employment and Social Development Act* and the *Employment Insurance Act*[1]. Applications for a SIN can be completed in person at Service Canada Centres (SCCs) or Outreach sites, through provincial birth registration, or by mail, depending on the applicant's eligibility. All SIN application information is retained in the Social Insurance Register (SIR) which is used by other authorized programs and departments to validate identity.

Audit Objective

The objective of this audit was to assess the adequacy of the SIN application process and the integrity of the SIR.

Summary of Key Findings

- The in person application process is well designed but opportunities exist to improve efficiency.

- The SIN@Birth model provides superior efficiency, client service, and data accuracy when compared to other SIN service delivery channels.

- Opportunities exist to exercise audit clauses with provincial partners to validate the reliability of information received via the SIN@Birth model.

- The SIN Program could enhance its quality monitoring (QM) activities to better target critical risks, compensate for processes with fewer controls, and achieve an integrated approach across service channels.

- Employee training, reference material, and support mechanisms are sufficient.

- Electronic validation with provincial and Citizenship and Immigration Canada (CIC) data sources results in a near error-free SIN application process. We noted that SIR data obtained prior to the implementation of existing rigorous controls requires enhancement.

- Authorized SIN partner program personnel have read-only access to more SIR records than required to complete their tasks. While user access reports are available, system access is not actively monitored.

---

[1] http://laws-lois.justice.gc.ca/eng/acts/h-5.7/FullText.html

Audit Conclusion

Overall, the SIN application process is adequate. There are opportunities to improve service delivery efficiency and effectiveness through expanding partnerships with CIC and implementing an integrated approach to QM. Additionally, data integrity within the SIR (specifically older data processed prior to the current validation model) requires enhancement, and SIR data access controls require strengthening.

Recommendations

1. In collaboration with federal partners, Integrity Services Branch (ISB) should assess the viability of a SIN application process based on the SIN@Birth model for applicants not born in Canada.

2. In partnership with the Citizen Service Branch (CSB), the regions and National Identity Services (NIDS), ISB should develop an integrated and risk-based national QM strategy for SIN transactions.

3. ISB should enhance historic SIR data where justified by cost-benefit analysis.

4. ISB should enhance SIR data access controls.

1.0 Background

1.1 Context

Introduced in 1964, the SIN is a nine-digit number used as a file identifier or account number for a variety of Government of Canada benefits and services. The SIN plays a vital role in the sound management and integrity of Government programs and services. All information related to each SIN record, including the personal information provided by clients in support of their SIN application, is housed in the SIR. The SIR is also used by other authorized programs and departments to validate identity.

The SIN is the responsibility of ESDC as legislated by *the Department of Employment and Social Development Act* and the *Employment Insurance Act*. Administration of the SIN and maintenance of the SIR are the responsibility of the SIN Management Services (SMS) unit within ISB. Over 1.4 million SIN transactions were processed in the fiscal year (FY) 2014–15[2]. The CSB is responsible for service delivery of the SIN at SCCs via the Social Insurance Number Rapid Access (SINRA) application which accounts for about 73% of total transaction volume. NIDS (based in the Atlantic Region) is responsible for processing complex applications and transactions, conducting QM of in person transactions, and providing phone support to both the public and ESDC employees. NIDS also processes applications received by mail which have declined significantly in recent years following the revision of mail-in eligibility requirements. Parents of newborns can use the Newborn Registration Service (SIN@Birth) which accounts for 24% of total transaction volume (and accounts for 37% of all newly issued SINs) and is administered by the participating provinces.

1.2 Audit Objective

The objective of this audit was to assess the adequacy of the SIN application process and the integrity of the SIR.

1.3 Scope and Methodology

The scope of this audit included a review of operational processes and service delivery channels supporting the SIN application process as well as processes and protocols supporting SIR data integrity. In addition to audit activities at National Headquarters (NHQ), regional visits were undertaken to review SIN operations in Bathurst, New Brunswick as well as front-end service delivery processes at SCCs across all ESDC regions.

The audit used a number of methodologies including document review, interviews, on-site observations, process walkthroughs, as well as sampling and testing of SIR data.

---

[2] Processing Statistics (monthly) 2014–2015: http://servicecanada.prv/eng/isb/integrity/sin-sir/report/results/050_020.shtml

2.0 Audit Findings

2.1 The in person SIN application process is well designed, but there are opportunities for greater efficiencies and expanded controls

When an applicant visits a SCC to apply for a SIN, they are greeted by a Citizen Service Officer (CSO) at the "Welcome Zone" who confirms their eligibility and determines whether they have the proper documentation to apply. The applicant subsequently waits in a queue to be called to the "Citizen Service Zone" where the SIN is processed by another CSO using the SINRA. The CSO then authenticates the applicant, verifies the authenticity of the applicant's identification documentation, and enters their biographical data into SINRA. The applicant then verbally confirms their personal information and provides their address and phone number. During the interaction, the CSO is alert to any risk factors that may warrant additional examination or referral to NIDS or an investigator. If no red flags are triggered and the SINRA verifications confirm the applicant's information, the CSO completes the application process and provides the applicant with a paper printout of their SIN.

We found that in most instances the SINRA process is well controlled to limit errors and support the integrity of the SIR. The SINRA web application is a step by step process that must be adhered to in order to issue a SIN. The application contains built in controls that limit the likelihood of errors. For example, a wide variety of system messages minimize the risk of inappropriate actions. They range from attention messages which require the CSO to verify the information and either change the data or deem the situation is valid, to error messages which prevent the CSO from continuing the application until inaccurate data is changed or another appropriate action is taken. System messages also flag complex or risky applications that must be forwarded to NIDS or an investigator. In addition, as part of the 2014 Internal Audit of the Departmental Information System and Technology Controls, audit testing demonstrated that data input controls for new information entered in the SIR were operating effectively.

Safeguarding personal information and process efficiency

Only one of the six offices we visited was using a password-protected printer code to retrieve the SIN confirmation letter from the shared printer. We were informed that privacy breaches have occurred in the past whereby an officer provided an applicant a SIN confirmation letter belonging to someone else that was applying at the same time. Given that similar findings have been identified in past audits, we would suggest that CSB require all regional SCCs to use printer codes to retrieve printed SIN letters from shared network printers.

Unlike other application processes in ESDC, the majority of SIN applications are facilitated verbally in a SCC. In most offices, the client verbally provides personal information to the CSO in an open concept layout thereby creating the potential risk of personal information being overheard. Utilizing white noise as is done in some SCCs is a possible risk mitigation technique that we have observed which could be adopted by all SCCs.

Alternatively, the current verbal process could be revised to require the applicant to type the required information using the existing computer workstations situated in the "Self-Help Zone" of a SCC. SCCs have established a 25 minute wait-time service standard for applicants after checking into the "Welcome Zone" prior to beginning the SIN application process with a CSO. An opportunity exists to better use this wait-time by having the applicant enter the required personal information into a secure application on a computer terminal within the SCC. This approach would also allow the application privacy statement to be provided and accepted electronically with a digital acceptance signature. Once completed, a CSO in the "Citizen Service Zone" would authenticate the applicant using established techniques to identify red flags (referring applicants to an investigator where appropriate), perform electronic validation, and finalize the transaction. This approach could reduce SIN interaction times, improve process efficiency and enhance accuracy of data that is not validated with the provinces or CIC.

Authentication of documents and identification of applicants

The most important control in the SIN process is the authentication of identity documentation which has been significantly improved through implementing electronic validation with source data. Online validation of birth certificates is currently available in nine provinces with an agreement in place with the remaining province to implement electronic validation in early 2016. In addition, most citizenship and immigration documents can be validated with source data using a CIC system. Electronic validation provides several benefits to the SIN application process: it confirms that documentation presented is government issued and valid, it reduces the likelihood that multiple SINs will be issued to an individual, and it ensures that key SIN information, such as name and date of birth, are exact matches to the Provincial or CIC issuing authority source documentation. The importance of having SIR data that matches the source has increased over time as the SIR has become more relied upon as the Government of Canada source of identity information. It should be noted however, that some SIR data fields collected during the application process (e.g. names of parents which is used to authenticate clients) are not validated with provincial or CIC source data.

While electronic validation of identity documentation is a significant improvement, it does not confirm that the individual applying is the rightful owner of the document. Although a universal solution may not be feasible due to the varying ages of applicants, requiring government-issued photo identification could provide better assurance of the applicant's identity, thereby reducing the risk of identity theft.

In both FYs 2013–14 and 2014–15, program statistics revealed that electronic validation was performed on 89% of all processed applications. To assess the impact that electronic validation has on error rates, the audit team extracted a random representative sample of SIN applications processed between 2008 and 2015 where the data was not validated electronically with source data. After performing electronic validation of the records against CIC or provincial data, we concluded with a 95% level of confidence that over 8% of the sample's population had at least one error in the data elements that would have otherwise been confirmed and corrected through electronic validation. While most of these errors would not result in inaccurate payments (including incorrect sex or misspelling of the surname or given name), such errors could cause future delays for SIN holders when accessing government programs and increase operational costs for SIN-enabled programs. Of note, only 2 files (out of our sample of 92) were related to Date of Birth errors, which could result in an overpayment. Our file review results underscore the importance of the electronic validation control.

Since electronic validation is such a critical control and results in a near error-free SIN application process (assuming the provincial or CIC source data is accurate), it is expected that compensating controls would exist to limit the risk of errors in situations where electronic validation is not performed or possible. However, we did not identify sufficient compensating controls that specifically target cases when electronic validation is not performed with the provinces or CIC. When provincial validation systems are temporarily unavailable, SINs will continue to be issued in SCCs. This resulted in 2,500 transactions (about 0.25%) being processed while the provincial validation systems were unavailable during the FY 2013–14. While applicant data is later sent by batches for validation, **PROTECTED**, leaving easily correctable errors in the SIR. Alternatively, CSOs could scan and email identity documents to NIDS when the validation portal isn't working, and a NIDS agent could then review any non-matches using the scanned identity documents allowing for easy correction of data entry errors. In rare cases where they suspect that the identity document is invalid, they could proceed to flag the record for investigation.

Dormant SIN reversals

Each year, the Canada Revenue Agency (CRA) provides ESDC with a list of SINs that are associated with **PROTECTED**. ESDC then matches those SINs to records in the SIR and places a "dormant" flag onto that file. Until it is removed, the dormant flag may prevent the SIN holder from receiving benefits from some SIN authorized programs. To remove the flag, the client must visit a SCC where a CSO will ask the client to fill out a questionnaire which will be sent to NIDS for processing. An officer in NIDS will then evaluate whether it is a simple request or a suspicious request using a risk chart, and suspicious requests will be subsequently addressed by the contact centre. In 2014–15 there were 75,556 new dormant flags and 10,889 dormant flag reversals. To streamline the processing of these transactions, CSOs could process non suspicious dormant flag removal requests after validating the identity of the individual. Not only would this be more efficient but it would provide better service for clients requesting routine dormant reversals.

2.2   Cost savings and data accuracy enhancements could be achieved

The SIN Program has entered into service delivery partnerships with the governments of nine provinces to permit parents of newborn babies to simultaneously complete their child's birth registration with the province and also apply for their SIN. In FY 2014–15, just over 346,000 SINs were issued through SIN@Birth which represented about 94% of the birth registrations in those provinces and 37% of all new issued SINs. Each SIN issued through the SIN@Birth model carried a transaction cost of $1 paid to the province for facilitating the application process. This stands in contrast to the SCC transaction cost of $13 per SIN transaction. The service model is not only more convenient for Canadians, but it also provides cost savings to the Department by leveraging a unified application with the provinces when registering new babies. Moreover, possible data entry errors within the current SCC process for data elements not currently validated through electronic validation (e.g. names of parents) are eliminated as the SIN data precisely matches provincial birth information within the provincial vital statistics databases.

While SIN@Birth controls have been effectively designed, program management has not sought assurances from the provinces to confirm that their controls are functioning as intended. Audit clauses in the Memoranda of Understanding (MOUs) specify that provinces are to regularly conduct audits and provide the reports to ESDC. However, program management has neither requested any audits in the ten years since the first provincial agreement was signed nor are they aware whether any provinces have undertaken audits as outlined in the MOUs. Given the imperative for confidence in SIR data integrity and information management practices, combined with the transaction fees ESDC is paying for the service, it would be a good practice for the SIN Program to periodically exercise the audit clauses within the established provincial agreements.

Given the success of SIN@Birth, there is an opportunity to expand the existing model for applicants not born in Canada. Currently, the majority of these applicants must visit a SCC to apply for a SIN. If these applicants could simultaneously apply for a SIN as part of the application process for CIC documentation and when necessary complete the process upon arrival at customs in Canada, it would result in substantial annual savings, enhanced client service, and improved data accuracy. In the 2014–15 FY, as many as 560,000 SIN applications could have been processed through this model, representing possible annual savings of $7 million. We recognize that it is unlikely that a similar SIN@Birth cost per transaction would be levied by federal partners and are also aware that it would require significant initial investment to transition to the model. For comparative purposes, ESDC's investment cost to establish the partnership with Ontario was about $5 million.

It should be noted that in the interim of establishing an automated solution in partnership with CIC, there have been some innovative regional projects launched to provide enhanced client service in partnership with CIC and Canada Border Services Agency (CBSA). SIN@Landing is a pilot project whereby ESDC partnered with CBSA to issue SINs to permanent residents when clearing customs at Pearson Airport in Toronto. Service Canada Officers are stationed at the airport to facilitate the provision of a SIN to these newly landed immigrants. Mass Landing is a partnership pilot launched in Montreal between ESDC and CIC whereby SINs are issued to new permanent residents. The granting of permanent residence is held within a Montreal-area SCC where the new permanent residents can immediately be assisted by an officer to obtain their SIN. While both the SIN@Landing and Mass Landing pilot projects are beneficial from a client service perspective, neither represents the same cost savings nor enhanced data accuracy opportunities that would be achieved through a fully developed service delivery partnership with CIC using the SIN@Birth model.

Recommendation

1. In collaboration with federal partners, ISB should assess the viability of a SIN application process based on the SIN@Birth model for applicants not born in Canada.

Management Response

ISB agrees with this recommendation, recognizing that a model similar to SIN@Birth for applicants not born in Canada brings with it the potential for both increased integrity and service for the program and this client group.

In order to assess the viability of such an approach, ISB will seek concurrence from senior management at CIC, and CBSA to establish a joint working group to study the possibility of this approach. If concurrence is received, the working group will report back to senior management in each department by November 2016 on the viability of a SIN application process based on the SIN@Birth model for applicants not born in Canada.

2.3   Weaknesses were identified in SIN quality monitoring

While there are several disparate mechanisms in place to monitor the quality of SIN processing and service delivery, some weaknesses were identified, including the lack of a holistic risk-based QM strategy. Limited effort has been made to optimize QM coverage across the SIN Program or revise parameters to reflect changing controls, and there is minimal collaboration between groups responsible for SIN QM initiatives.

NIDS, which operates within the Atlantic region, is responsible for responding to SIN phone enquiries, and processing both complex transactions as well as client applications received by mail. Their business expertise unit has created a QM program which reviews a random selection of applications processed by NIDS. Although many of these applications originated as referrals from SCCs, we were informed that feedback on results is neither provided to individual CSOs nor to management. In addition, weekly reviews are performed on transactions deemed to be critical and comprehensive bi-annual reviews are performed for all NIDS employees. While the design of the QM provides a balance between coverage, risk, and employee feedback, the process and review criteria have not been formalized, and resources are not dedicated to monitoring activities. We also noted that there may be greater opportunities to share results with NIDS management for continuous improvement purposes.

The SINRA QM reviews SIN applications that have been completed in SCCs. About 4% of total application volume is reviewed for critical errors (Legitimacy Reviews) and 10% of these files (0.4% of total volume) are also reviewed for adherence to procedures and data accuracy (Quality Reviews). In FY 2014–15 just under 40,000 Legitimacy Reviews were performed and in total, seven files contained critical errors, for an error rate of 0.02%. While the low error rate exemplifies the strong controls built into the SINRA application, it also demonstrates inefficiencies in current QM practices. For applicants using documentation that can be validated electronically, there are controls built into SINRA that practically eliminate the risk of a date of birth error or multiple SINs being issued to an individual. In FY 2014–15, about 11% of applications were not validated electronically. A risk-based QM strategy that places more emphasis on transactions where electronic validation has not been performed would add more value than the current random approach as these transactions carry a much higher risk of errors.

Quality Reviews provide more value than Legitimacy Reviews since about 5.5% of files contained an error which results in more feedback to CSOs and program management. However, there are opportunities to streamline the evaluation criteria as 14 of the 23 criteria did not register a single error in the previous FY. Revising and updating criteria to reflect current controls and processes would eliminate redundant review steps. There also appears to be a missed opportunity to use QM results to make process or training improvements given that the same top error has persisted for the past five years. Given that a CSO will spend about five to ten minutes to prepare and send the documentation for each of the 40,000 Legitimacy Reviews (4,000 of which are also reviewed for quality), it is important that the SINRA QM process targets risks and supports continuous improvement.

Since SINRA Quality Reviews are performed in Bathurst using SIR data and copies of documentation, it is not possible to perform a comprehensive evaluation of the in person elements of SIN interactions. The Agent Performance System (APS) was designed to enable the review of one SIN transaction per CSO (by their team leader) each month. The APS facilitates the evaluation of interactions with clients including applicant authentication and adherence to in person SINRA protocols. However, we found that despite its merits, the APS had only been implemented in one region. One of the reasons regions may be reluctant to adopt the APS is that the current staffing model in SCCs does not place emphasis on team leader expertise, which can create challenges when team leaders are evaluating their CSO's SIN transactions under the APS. While the APS currently requires that the team leader be a SINRA certified coach in order to perform the evaluations, it is our opinion that in depth "trainer-level" expertise would not be required to perform APS reviews. We would suggest that this requirement be revisited and if necessary, modified to ensure that all team leaders can obtain the necessary qualifications to allow the APS to be implemented nationally.

Recommendation

2. In partnership with CSB, the regions and NIDS, ISB should develop an integrated and risk-based national QM strategy for SIN transactions.

Management Response

ISB agrees with this recommendation. SMS will develop an integrated risk based QM strategy for tier 1 and 2 SIN issuance by December 2016. This will include a risk analysis and the development of appropriate QM measures to mitigate identified risks. Full implementation will be dependent on any system changes that may be required. If such changes are minimal, a new QM strategy will be implemented by June 2017.

2.4 Training and support for the SIN Program is sufficient, but there are opportunities to improve the efficiency of training activities

Discussions with both in person CSOs and NIDS employees confirmed that SIN reference material is complete and up to date. SINRA has reference material built into the system making it easily accessible for CSOs during client interactions, while NIDS employees have access to reference material on the ESDC intranet. If a CSO requires assistance in processing an application, a contact centre is available for immediate telephone support. Feedback from CSOs indicated that they rarely wait on hold and they are satisfied with the assistance provided. NIDS employees indicated that support is available on site or through business expertise.

Training for NIDS employees is a challenge due to the varying nature of the work. It is generally delivered on site by a co-worker or the business expertise unit and is complemented by monitoring and coaching. On the other hand, a sophisticated training and certification program is in place for in person service delivery. Once a CSO has demonstrated their ability to accurately complete ten SIN transactions to a certified SINRA coach, they will receive SINRA certification. Certification is mandatory for all CSOs that process transactions in SINRA, and a CSO must be re-certified following 120 days of inactivity.

Certification and re-certification are performed by a certified SINRA coach who is expected to be at least at the PM-03 level. Although we received mostly positive feedback regarding the quality of the training and certification program, there may be opportunities to improve efficiency. For example, requiring the coach to be at the PM-03 level means the task generally falls to Business Expertise Advisors (BEA) since team leaders do not normally possess the technical knowledge required. This often creates a need to travel since BEAs aren't situated in SCCs. Exploring alternatives such as virtual coaching or having team leaders assume the responsibility (as is the case in one region) may improve efficiency. Another alternative being employed by one region had CSOs performing the coaching in some cases. Although this isn't the typical approach, it didn't cause any observable issues as this region had the highest processing accuracy rate in FY 2014–15.

The SIN Program requires SIN re-certification if a CSO hasn't recently processed a transaction. However, there may be an opportunity to reduce costs by revisiting the length of time required before re-certification. We expected that the length of time would have been chosen to balance the cost of re-certification with the increasing risk that a CSO will make critical errors the longer they are inactive. We found that there wasn't any particular rationale for choosing 120 days as opposed to another length of time. Given that re-certification can be costly and SINRA has strong built in controls, we would suggest reassessing the length of time before re-certification and exploring lower cost re-certification options to ensure an optimal balance of risk and cost.

2.5 Improving **SIR** data accuracy is integral to enhancing its reliability for authorized **SIN** user programs

Controls supporting SIR data accuracy have gradually improved since the implementation of the SIN in 1964. For example, until 1976, SIN applicants were not required to provide identity documentation such as Birth Certificates or Citizenship Cards, meaning accuracy was dependent on the applicant providing the correct information. Data accuracy controls on application processing such as the implementation of electronic validation with provincial or CIC source data have significantly increased data reliability for recently issued SINs. As previously mentioned, our file review results demonstrate that in the absence of the electronic validation control being applied the likelihood of errors increases. SIR data has become more and more relied upon over time as a client identifier which creates a significant challenge when relying on data that was created before the advent of current controls. Consequently, **PROTECTED** for ESDC's pensions programs[3] which accounted for $79B in benefit payments in FY 2013–14[4].

Not all SIR errors carry equal risk; therefore, it is important to consider both the potential savings and costs associated with any improvement initiatives targeting SIR errors which occurred prior to the existing electronic validation controls. Incorrect payments are generally caused by critical errors such as the incorrect date of birth, a citizen with multiple SINs, or a citizen using the identity of a deceased or fabricated individual. These errors increase the risk of improper identity authentication and benefit calculations for the programs authorized to use the SIN. Less critical, but still costly, are errors in the client's personal information such as their name. These errors may cause an inconvenience to clients in delaying service as well as a cost to the SIN authorized programs to investigate and correct deviations. While these errors will hinder the ability to rely on the SIR to validate information, they are unlikely to result in payment errors.

---

[3] Canada Pension Plan, Old Age Security, Guaranteed Income Supplement, and Allowances.
[4] http://www.esdc.gc.ca/en/reports/dpr/2014/section2.page#s2.3.1.1

PROTECTED

A separate data analytics unit within ISB possesses the expertise and tools to perform econometric analyses and assist with data accuracy improvement initiatives. However, the unit currently lacks the capacity to adequately support a significant project to enhance SIR data quality. Moreover, SMS does not possess sufficient expertise or dedicated resources to perform this work. In the absence of resources to perform a comprehensive SIR improvement project, analytical resources have been directed towards tracking error rates, identifying anomalies, and performing targeted analysis of risky subsections of the SIR.

The SIN Program maintains five Key Performance Indicators (KPIs) that cumulatively form the estimated critical error rate in the SIR. Three of the KPIs are used to estimate the "Legitimate SIN Accuracy Rate" PROTECTED and is reported in the Department's Report on Plans and Priorities. The Legitimate SIN Accuracy Rate is an estimate of the error rates attributed to PROTECTED . The accuracy rate for this metric has consistently exceeded 99.9%.

The other two KPIs PROTECTED can be combined to provide the "Vital Events" error rate. These errors are considered critical as they can contribute to incorrect payments. The Vital Events error rate improved from 2.7% in 2007 to 1.9% in 2014. Part of this improvement stems from provinces providing PROTECTED . This is a good measure to improve SIR accuracy which has contributed to a reduction in the critical error rate. However, challenges remain in PROTECTED has also decreased as a result of the implementation of electronic validation which strengthens accuracy for new applicants, as errors are identified and corrected during interactions with Service Canada. However, these measures are not sufficient to correct data inaccuracies associated with older data.

Recommendation

3. ISB should enhance historic SIR data where justified by cost-benefit analysis.

Management Response

ISB agrees with this recommendation. We will work with Statistics Canada to gather information about the quality of the historical data and develop an action plan to address findings where the benefit is commensurate with the cost by June 2017.

2.6 Access controls to SIR data require strengthening

We found that processing officers from ESDC managed SIN-authorized programs, such as Employment Insurance and Canada Pension Plan, have full search capabilities of SIR data, rather than simply an ability to confirm information obtained from clients matches the SIR information. Given that the SIR is considered a foundational Government of Canada database and contains personal information on the vast majority of Canadians and many non-Canadians, we would expect strong data access controls be implemented.

Although audit trails exist to track and record SIR access by authorized users, and exception reports are produced, there is limited monitoring of SIR access patterns to verify whether there may be inappropriate access activity. Moreover, other SIN-authorized users **PROTECTED** . While safeguarding provisions are laid out in the **PROTECTED** , we have been informed that the Program has not undertaken any monitoring activities or exercised its audit clauses to verify that access is appropriately restricted, safeguarding protocols are followed and previous copies are properly disposed of **PROTECTED** .

As SIR data accuracy improves, there could be an opportunity to replace unrestricted SIR data search access with a data validation portal similar to the provincial model. This may require a sizeable investment but it could enhance the integrity of the SIR. Notwithstanding future possible enhancements, compensating controls should be strengthened to ensure SIR data is accessed appropriately.

Recommendation

4. ISB should enhance SIR data access controls.

Management Response

ISB agrees with this recommendation to improve the monitoring of system access. The SIN program has in place processes to ensure that access to the SIR is restricted to those who need such access. Work is underway following a recent Audit of the Departmental Information System and Technology Controls which recommended an evaluation of the feasibility of a departmental approach to actively monitoring high risk systems access. Any changes made as a result of this work will be taken into account as the SIN program improves its data access controls.

Actions are expected to be completed by August 2017.

2.7 Staffing challenges exist for the national support unit which could impact the ability to address some Program risks

The SMS unit is critical for ensuring the security and integrity of the SIN issuance process and maintaining the accuracy and completeness of the SIR. It is currently co-located in NHQ and Bathurst, with many key employees residing in Bathurst. In 2014, it was announced that the group would transition to operate exclusively out of NHQ. While this consolidation will result in greater efficiencies and allow the integrated group to more effectively target resources to needed program enhancements, several risks must be mitigated to ensure a smooth transition and to avoid any potential operational disruptions.

Some of the most critical job functions and the associated program knowledge and expertise are currently performed by employees in Bathurst who are not planning on moving to NHQ. New employees will need to be trained by existing individuals who will also be expected to continue performing their regular job duties. In addition, roles and responsibilities for some positions have yet to be defined, creating the risk that key functions may not be effectively and efficiently performed following the transition. Information management was also identified as a weakness that could exacerbate these issues. If not properly mitigated, these risks could not only threaten the ability of SMS to carry out its operational support role, but also jeopardize its ability to implement enhancements to service delivery models and to SIR data integrity.

3.0 Conclusion

Overall, the SIN application process is adequate. There are opportunities to improve service delivery efficiency and effectiveness through expanding partnerships with CIC and implementing an integrated approach to QM. Additionally, data integrity within the SIR (specifically older data processed prior to the current validation model) requires enhancement, and SIR data access controls require strengthening.

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 Audit of the Management and Delivery of the Social Insurance Number Program. 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

Audit Criteria	Rating
SIN Application Process	
• The process is risk-based, efficient, well communicated and consistently applied.	◉
• Established guidelines, training and tools are sufficient, understandable and comply with policy and legislative requirements.	●
• Oversight, quality assurance, and feedback mechanisms are established to monitor performance and trends, and enable continuous improvement.	◉
• Applicants are adequately authenticated and personal information is appropriately safeguarded to maintain program integrity in accordance with departmental standards.	●
• Appropriate staffing strategies are in place to efficiently manage operations and effectively mitigate risk.	◉
SIR Integrity	
• Protocols, agreements and communication mechanisms are in place to support data accuracy and integrity.	◉
• Agreements, controls and communication mechanisms are in place to limit SIR data sharing and access in accordance with legislation.	◉

✪ = Best practice
● = Sufficiently controlled, low risk exposure
◉ = Controlled, but should be strengthened, medium risk exposure
○ = Missing key controls, high risk exposure

Appendix B: Glossary

APS   Agent Performance System

BEA   Business Expertise Advisor

CBSA   Canada Border Services Agency

CIC   Citizenship and Immigration Canada

CRA   Canada Revenue Agency

CSB   Citizen Service Branch

CSO   Citizen Service Officer

ESDC   Employment and Social Development Canada

FY   Fiscal Year

KPI   Key Performance Indicator

MOU   Memoranda of Understanding

NHQ   National Headquarters

NIDS   National Identity Services

QM   Quality Monitoring

SCC   Service Canada Centre

SIN   Social Insurance Number

SINRA   SIN Rapid Access

SIR   Social Insurance Register

SMS   SIN Management Services

Appendix C: Types of SIR Errors

Personal Information Errors: Errors in these fields may reduce Service Canada's ability to validate identity of existing SIN holders for changes/updates to SIN data.

- Date of Birth (day) (inaccurate error)

- Place of Birth

- Current or Original Surname (full legal name) Current First Given Name or Original First Given Name

- Current Second Given Name or Original Second Given Name

- Gender

- Mother's Maiden name

- Father's First name

- Birth Certificate Registration Number

- Immigration ID

- Expiry date of 900 SIN

Critical Errors: Errors in these fields increase the risk of improper identity authentication and benefit calculations for the programs authorized to use the SIN.

- **PROTECTED**

- **PROTECTED**

- **PROTECTED**