Employment and Social Development Canada
Emploi et Développement social Canada

Unclassified

Audit of Identity Management Practices

June 2019

Internal Audit Services

Audit of Identity Management Practices

This publication is available for download at canada.ca/publicentre-ESDC .
It is available upon request in multiple formats (large print, MP3, braille, audio CD, e-text CD, DAISY or accessible PDF), by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. : Em20-138/2020E-PDF
ISBN: 978-0-660-31332-0

ESDC
Cat. No. : SP-1218-01-20E

TABLE OF CONTENTS

1. BACKGROUND

1.1 Context

Identity management is the process by which the Department determines whether the identity of an individual or organisation with whom it is transacting is legitimate. Adequate and consistent identity management practices mitigate the risks related to identity theft, the fraudulent use of identity documents, the improper granting of entitlements, the inappropriate allocation of benefits and services, financial losses to affected parties and the breach of an individual's right to privacy.

Pursuant to the Treasury Board’s Directive on Identity Management, the Department adopted an Identity Management Policy in April 2011, which was updated in April 2016. Supporting the departmental policy are the Identity Assurance, Evidence of Identity and Business Identity Validation standards. These standards are based on the Pan-Canadian Assurance Model that aims to achieve a “seamless, cross-jurisdictional, user-centric and multi-channel service delivery experience for all Canadians.”

These standards are meant to outline a framework for assessing the identity assurance needs of programs and services, and set the minimum information and process requirements for achieving the required levels of identity assurance within the existing legal authorities. Furthermore, identity management practices for programs and services must be developed to ensure alignment with the assurance level requirements for registration, authentication and validation.

Identity management practices broadly fall in the following processes:

- **Registration** is the collection of identity attributes for a specific service or program objective (e.g. name, date of birth, gender, Social Insurance Number, Business Number).
- **Authentication** is establishing confidence in the validity of an identity claim or credential submitted in support of an identity claim; that is, an identity claim made by a client or representative (of an individual or organisation) is determined to be true.
- **Validation** is verifying an identity claim of a client or representative (of an individual or organisation) who has provided identity information to the Department, or to an organisation delivering a service or program on its behalf, each time a client seeks to access a departmental service or program. This is to be achieved by confirming identity attributes with a valid and valuable source.

The development of identity management practices (including tools and procedures) is supported by advice, tools and guidance from Integrity Services Branch’s (ISB) Identity Policy and Programs Directorate.

1.2 Audit Objective

The objective of this audit was to determine if identity management practices:

- Have been developed, implemented and are consistent across programs and service delivery channels; and
- Adequately support the integrity and security of programs and services by adopting a risk-based approach to identifying individuals, businesses or organisations.

1.3 Scope

The scope of this audit included key departmental structures, processes and practices pertaining to the management of identity for a risk-based selection of programs and services with varying identity assurance needs. Identity management for individuals as well as businesses and organisations were included in the scope of this audit.

1.4 Methodology

The audit was conducted using a number of methodologies including:

- Documentation review and analysis;
- Interviews with management and staff from ISB's Identity Policy and Programs Directorate;
- Interviews with key identity management stakeholders for the selection of programs and services included in the audit scope; and
- Interviews and on-site walkthroughs in all four regions including testing of implemented identity management practices.

2. Audit Findings

2.1 Departmental policies and standards have not resulted in consistent identity management practices

Identity Management for Individuals

Internal Audit reviewed identity management practices for individuals across the following selection of programs:

- Employment Insurance (EI) Program
- Canada Pension Plan (CPP) Program
- Old Age Security (OAS) Program
- Social Insurance Number (SIN) Program
- Apprenticeship Grants (AG) Program
- Wage Earner Protection Program (WEPP)
- Parents of Young Victims of Crime (PYVC) Program
- Canada Education Savings Program (CESP)
- Canada Disability Savings Program (CDSP)
- Canada Student Loans Program (CSLP)

Over the course of 2014, 2015 and 2016, all of these programs underwent a departmental assessment to determine if their identity management practices met policy requirements. Out of the 10 programs, only EI and OAS fully complied with the identity standards. The remaining 8 programs identified gaps, mostly related to the collection and validation of clients' mother's family name at birth and client status (i.e. Canadian citizenship, Aboriginal or Foreign status). Citing costly system changes, privacy implications and sufficient compensating controls, 7 out of the 8 programs opted for the status quo and did not modify their identity management practices. This preserved the inconsistencies that existed prior to the creation of the departmental policy.

Following those assessments, in April 2016, the Department updated its identity management policy and related standards to allow for more flexibility. For example, in the updated standards, identity attributes are now to be collected "within the limits of each individual program's respective authorities" and the mother's family name at birth "could be collected […] when applicable or if required". Current identity standards for individuals adopt a non-prescriptive tone and allow for interpretation which might explain the inconsistent identity management practices across the Department.

Furthermore, the policy and standards remain vague on going above requirements. For example, for returning clients, the departmental standard mandates a minimum of three identity attributes that need to be provided by the client. Internal Audit's fieldwork has shown that all programs use more than the minimum, some programs using six identity attributes to validate the identity of clients.

The absence of a departmental approach to identity management of third party representatives also resulted in inconsistencies observed by Internal Audit during our fieldwork. The current standard acknowledges this shortcoming and mandates programs to determine their own requirements for recognition of someone claiming to represent a client, based on their respective authorities.

Although consistency and a seamless service experience are mentioned repeatedly in the Department's identity management policy (both as principles and expected results), Internal Audit's fieldwork observed fragmented practices that lead to inconsistent user experience when accessing the Department's programs, benefits and services.

Identity Management for Organisations

As part of the April 2016 update to the Department's identity management policy, a business identity validation standard was created to "ensure program integrity as well as the service experience of organisations." Internal Audit has reviewed the standard and concludes that the tone is prescriptive enough to achieve the expected consistency if programs comply with the standard.

Recommendation

1. ISB should review the current Identity Management Policy and its related standards to use a language that is prescriptive enough to achieve the expected consistency across program and delivery channels, especially as it relates to third party representatives.

Management Response

*ISB agrees with this recommendation. While a degree of flexibility is required to accommodate individual program authorities, consistent identity management practices are expected to ensure seamless service delivery. ISB will undertake a review of the Identity Management Policy to strengthen the requirement language and limit interpretation, in particular to the requirements for **PROTECTED**.*

Actions are expected to be completed by September 2020.

2.2 Current identity management practices for individuals can be improved to adequately support program integrity

Internal Audit reviewed identity management practices for individuals across the following selection of programs and noted the following:

- **EI Program**: The EI program registers and authenticates individuals adequately to support program integrity. **PROTECTED**. Client identity is adequately validated whether they contact the Department in person, over the phone (EI call center or EI processing centers) or online through their My Service Canada Account (MSCA).
- **CPP and OAS Programs**: The CPP and OAS programs register and authenticate individuals adequately to support program integrity. **PROTECTED**. Client identity is adequately validated when they contact the Department in person, through pensions call centers and online through MSCA. However, because of the lack of clear guidance and monitoring, Internal Audit cannot conclude that clients' identities are adequately validated by pension processing centers whether it be on outgoing or incoming calls.
- **SIN Program**: The SIN program registers, authenticates and validates individuals adequately to support program integrity **PROTECTED**.
- **AG Program**: The AG program registers and authenticates individuals adequately to support program integrity. **PROTECTED**. Client identity is adequately validated when they contact the department in person. However, because of the lack of clear guidance and monitoring, Internal Audit cannot conclude that clients' identities are adequately validated by AG processing centers whether it be on outgoing or incoming calls.
- **WEPP**: The WEPP registers, authenticates and validates individuals adequately to support program integrity and fully complies with the departmental Identity Management Policy. However, if the client contact WEPP officers by phone, they will have to provide six elements to validate their identity, double what the departmental policy requires. There is an opportunity to standardise this process to increase consistency.
- **PYVC Program**: The PYVC program registers, authenticates and validates individuals adequately to support program integrity and fully complies with the departmental Identity Management Policy.
- **CESP, CDSP and CSLP**: The CESP, CDSP and CSLP register, authenticate and validate individuals adequately to support program integrity and fully comply with the departmental Identity Management Policy.

Recommendation

2. ISB should periodically monitor departmental programs to confirm that consistent and sufficient identity management practices have been implemented.

Management Response

ISB agrees with this recommendation and had already obtained consultant services, in the winter of the 2018–19 fiscal year, to develop options for a monitoring and reporting strategy to address this issue. ISB will continue to explore these options and engage with program areas to put a reporting schedule into place that would help ensure that programs have fully implemented consistent identity management practices.

Actions are expected to be completed by September 2020.

2.3 Current identity management practices for organisations need to be strengthened to adequately support program integrity

Internal Audit reviewed identity management practices for organisations across the following selection of programs and noted the following:

- **Job Bank**: Job Bank uses an online-only portal for users to create an account and post job offerings on behalf of their organisation. Current identity management practices mostly comply with the standard. To fully comply, Job Bank should also request legal documents proving the existence of the organisation when dealing with them for the first time. Additionally, correspondence from the organisation recognising the individual as their representatives should also be requested.
- **EI Program – Records of Employment (ROE)**: ROEs are key documents produced by employers and are required to claim EI benefits. Paper ROEs can be ordered by phone. To do so, an individual calls the Employer Contact Center and provides the business number, legal name and address of the organisation for which they would like to receive ROEs. This information is validated against the Canada Revenue Agency's records and upon validation, the order is placed. **PROTECTED**. ROE can also be completed online through ROE Web. Current identity management practices for ROE Web comply with the standard. As of October 2018, 90% of ROEs were completed online.
- **Canada Summer Jobs (CSJ) Program**: The program provides wage subsidies to employers from not-for-profit organisations, the public sector, and private sector organisations with 50 or fewer full-time employees. Employers can apply for the wage subsidy using a paper form (submitted by mail), using an online interactive form or using the Grants and Contributions Online System (GCOS, discussed below). The process for authenticating and validating the organisation and its representative is the same for mailed-in paper forms as for online-submitted forms. **PROTECTED**.
- **New Horizon for Seniors Program (NHSP)**: The program funds community-based projects with a grant of up to $25,000 per year, per organisation. As for CSJ, NHSP projects can be submitted using a paper form (submitted by mail), using an online fillable form or using GCOS. **PROTECTED**.
- **Grants and Contributions Online System**: Both Grant and Contribution programs reviewed (CSJ and NHSP) allow applications to be submitted through GCOS. Current identity management practices for GCOS comply with the standard. Unfortunately, only a small percentage of applications (less than 10%) were submitted using GCOS in 2018.

Recommendation

3. ISB, in collaboration with program areas, should review identity management practices for organisation to address compliance gaps with departmental and government identity standards. **PROTECTED**.

Management Response

ISB agrees with this recommendation and confirms that there is a gap in the implementation of the Identity Management Policy for ***PROTECTED*** *as they had been requested to pause the development of their gap analyses and implementation plans until after the Department became* ***PROTECTED****. Recent amendments to the Department of Employment and Social Development Act for service delivery have resolved this issue.*

The Treasury Board Secretariat is expecting to renew the Directive on Identity Management in 2019. ISB will work with ***PROTECTED*** *to address any gaps in their identity management practices and/or update the Policy as necessary. Preliminary contact has already been made with* ***PROTECTED*** *to provide identity management guidance.*

Actions are expected to be completed by March 2022.

3. Conclusion

The audit concluded that identity management practices have been developed, implemented but have not achieved the expected level of consistency across programs and service delivery channels. These consistency issues mainly stem from programs that use a higher standard than required by the policy and from a lack of a departmental approach to handling individual clients’ third party representatives.

Overall, identity management practices for individuals adequately support the integrity and security of programs and services. Exceptions have been identified for each program where enhancements could be made to further increase the integrity of programs.

PROTECTED

4. 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 identity management practices of the programs listed in this report. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

APPENDIX A: AUDIT CRITERIA ASSESSMENT

Audit Criteria		Rating
It is expected that the Department developed adequate policy, standards, tools and guidance that enable the development of consistent identity management practices by departmental programs and services.		◉
It is expected that the Department monitors developed identity management practices to confirm that policy requirements are met.		◉
It is expected that programs and services implemented (i.e. designed, documented and communicated) identity management practices that align with the assurance level requirements for registration, authentication, validation and modifications.	Identity management practices for individuals	◉
	Identity management practices for organisations	◉
It is expected that programs and services secure identity information from unauthorized access.		●
It is expected that programs and services monitor identity management activities to confirm that remedial actions are taken on a timely basis to address gaps impacting program integrity.	For all channels (in-person, specialised call center, mail, online) except processing center	●
	Processing centers incoming and outgoing calls	◉

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

Appendix B: Glossary

AG	Apprenticeship Grants
CDSP	Canada Disability Savings Program
CESP	Canada Education Savings Program
CPP	Canada Pension Plan
CSJ	Canada Summer Jobs
CSLP	Canada Student Loans Program
EI	Employment Insurance
GCOS	Grants and Contributions Online System
ISB	Integrity Services Branch
MSCA	My Service Canada Account
NHSP	New Horizon for Seniors Program
OAS	Old Age Security
PYVC	Parents of Young Victims of Crime
ROE	Records of Employment
SIN	Social Insurance Number
SIR	Social Insurance Registry
WEPP	Wage Earner Protection Program