



Auditor General

MANITOBA

Report to the Legislative Assembly

Vital Statistics Agency

Independent Audit Report

Website Version



September 2020

This page is intentionally left blank.



September 2020

The Honourable Myrna Driedger
Speaker of the House
Room 244, Legislative Building
450 Broadway
Winnipeg, Manitoba R3C 0V8

Honourable Ms. Driedger:

It is an honour to submit my report titled, *Vital Statistics Agency*, to be laid before Members of the Legislative Assembly in accordance with the provisions of Section 28 of *The Auditor General Act*.

Respectfully submitted,

Original Signed by:
Tyson Shtykalo

Tyson Shtykalo, CPA, CA
Auditor General

This page is intentionally left blank.

Table of contents

Auditor General's comments	1
Report highlights	3
Main points	5
Response from officials	11
Background	13
Audit objectives, scope and approach	15
Criteria	16
Findings and recommendations	19
1 Weak identification and management of security and privacy risks	19
1.1 No comprehensive risk management processes	19
1.2 Privacy impact assessments not conducted	20
1.3 Inadequate physical protection of documents and office premises	21
1.4 Weak information security controls	24
1.5 Weak processes for sharing information with other government organizations and individuals	30
2 Weaknesses in the controls that ensure information integrity	32
2.1 Processes to ensure accuracy of events registry need improvement	32
2.2 Controls in place to ensure complete and accurate certificates issued	36
3 Certain policies, procedures and guidelines needed to be documented, or reviewed and updated	37
3.1 Gaps in the development of policy instruments	37
3.2 Existing policy instruments not reviewed and updated	38
Conclusion	39
Additional information about the audit	41
Summary of recommendations	43

This page is intentionally left blank.

Auditor General's comments

The Vital Statistics Agency plays a critical role in Manitoba, holding nearly four million records of vital events since 1882 — including births and deaths.

All Manitobans have a vested interest in ensuring this information is properly protected against unauthorized access, use, disclosure or destruction. Failure to offer these protections could compromise the integrity of the information, and create significant privacy concerns.

In this audit, we found several weaknesses in the way the Agency was managing vital events information.

We found the Agency's information security controls — which protect information and information systems against unauthorized access or modification — were in need of improvement. We noted the Agency did not regularly review staff access to registry software. Periodically reviewing users' access rights, and withdrawing unneeded access, ensures access to information is appropriately restricted. Weak access controls continue to be a challenge in other government departments as well, as we had noted in our 2018 report, *Audit of eChart Manitoba*.

We also noted some weaknesses in the physical security controls intended to protect vital events certificates and documents at the Agency's office. We found, for example, inadequate separation between work and public areas, and noted fire inspections were not conducted regularly.

I was encouraged to see the Agency had controls in place to ensure vital events certificates accurately reflected the information found in the vital events registry. However, the processes to ensure the accuracy of the registry information needs improvement.

This report includes 19 recommendations for improvements for managing the security, privacy risks and integrity of vital events information. Our first follow-up of these recommendations will be as at September 30, 2021. I would like to thank the management and staff members of the Vital Statistics Agency, other government staff, and event registrars that we met and interacted with during the audit for their cooperation and assistance. I also would like to thank my audit team for their diligence and hard work.

Original Signed by:
Tyson Shtykalo

Tyson Shtykalo, CPA, CA
Auditor General



This page is intentionally left blank.

Report highlights

Vital Statistics Agency

is a special operating agency within the Department of Finance.

Primary function:

Registers vital events and provides documents as proof of those events

Includes births and deaths

Holds nearly **4 million** records since 1882



Audit looked at the security, privacy and integrity of vital events information

What we found

Weak identification and management of security and privacy risks

Inadequate physical separation between work and public areas

Information security weaknesses

Staff access to registry software not regularly reviewed

Information not classified by level of sensitivity or importance

Secure mail not always used for delivering certificates and registration forms

Weaknesses in controls that ensure information integrity

Identity of event registrars not validated

Complete list of event registrars not maintained

Delays in registering some vital events

Deaths not always linked to births

No training for event registrars

Sensitive security findings were presented directly to management



Report includes 19 recommendations



This page is intentionally left blank.

Main points

What we examined

The Vital Statistics Agency (the Agency) holds a significant amount of personal and sensitive information about Manitobans that should be well protected and used effectively and efficiently in the course of its operations. We wanted to determine whether the Agency was properly managing the security and privacy risks associated with vital events information, and properly managing the integrity of vital events information. To do this we examined the controls related to information protection and information integrity for registrations of births, deaths, adoptions, name changes, and changes of sex designation.

What we concluded

We concluded that the Agency was not properly managing the:

- Security and privacy risks associated with vital events information.
- Integrity of vital events information.

As a result, control improvements are needed.

What we found

Our report has 19 recommendations. A summary of our findings is provided below. Additionally, we presented some sensitive findings and recommendations to management in an internal letter.

1 Weak identification and management of security and privacy risks

The Vital Statistics Agency (the Agency) holds a significant amount of personal information about Manitobans. There is a risk that the confidentiality and privacy of this information could be compromised, therefore, protecting the information from unauthorized access is critical. To determine if the Agency was properly managing the risks associated with the information, we looked at its processes related to vital events registration, information sharing, and certificates issuance. We then assessed whether the Agency had implemented effective controls to mitigate the significant risks.

In this section, we identify the following concerns with regard to protecting the confidentiality and privacy of vital events information:

- 1.1 No comprehensive risk management processes.
- 1.2 Privacy impact assessments not conducted.
- 1.3 Inadequate physical protection of documents and office premises.
- 1.4 Weak information security controls.
- 1.5 Weak processes for sharing information with other government organizations and individuals.

1.1 No comprehensive risk management processes

A risk assessment identifies events that could cause harm to an organization, how likely those events are to happen, and the potential impacts of the events. With this information, management can decide what controls are necessary to mitigate those risks.

We found that the Agency had not conducted a comprehensive risk assessment of its environment, nor had it implemented risk management processes.

1.2 Privacy impact assessments not conducted

The Agency maintains a significant amount of personal information about Manitobans, including information on births, deaths, adoptions, and sex designation changes. Protecting this personal information from unauthorized access and disclosure is critical and required by the *Freedom of Information and Protection of Privacy Act*. A privacy breach affects both the Agency and the individuals whose information is compromised. The Agency's reputation would be damaged and there may be financial implications and legal obligations as well. An individual whose information is compromised may experience physical safety risks, identity theft, loss of business or employment opportunities and damage to reputation or relationships.

We found privacy impact assessments were not conducted to identify the potential impacts if vital event information was compromised.

1.3 Inadequate physical protection of documents and office premises

Physical security controls are designed to prevent unauthorized access and to protect personnel from harm and property from damage. Insufficient or poorly designed and implemented physical security controls diminish the ability to protect personal information and vital event certificates.

We found weak physical security and environmental controls.

1.4 Weak information security controls

Information security is the protection of organizational information and information systems against unauthorized access or modification. Information security controls protect confidentiality, integrity and availability of computer system data.

The internet enables organizations and individuals to connect to information systems around the world. While this connectivity is a key enabler for organizational success, it also creates an avenue for cyber-hackers to gain unauthorized access to information systems. A determined hacker with the necessary skills, knowledge, and time can compromise computer systems and steal data from anywhere in the world. Numerous information security incidents related to viruses, worms, ransomware and other malicious software that compromise information systems occur daily worldwide and the frequency is only increasing. No organization, big or small, public sector or private, is completely safe from cyber-attacks.

We found:

- No periodic reviews of users' access rights.
- Registry software was not configured to segregate some conflicting roles and responsibilities.
- Privileged users' activities were not monitored.
- Shared accounts used.
- Information not classified by level of sensitivity or importance.
- Some sensitive weaknesses in information security controls.

1.5 Weak processes for sharing information with other government organizations and individuals

The Agency shares vital events information with various federal and provincial government departments and provincial vital statistics agencies. Information is shared with those organizations for purposes such as:

- Policy development.
- Confirming eligibility for public programs and benefits.
- Reporting out-of-province deaths.

The Agency also shares vital events information with authorized individuals. For example, a person whose birth is registered with the Agency can request a copy of their birth certificate.

It is important to sufficiently protect personal information from inappropriate access and disclosure.

We found:

- Mutual information sharing responsibilities not always defined.
- Secure mail not always used for delivering certificates and registration forms.

2 Weaknesses in the controls that ensure information integrity

It is important to ensure that the Agency's events registry is complete, accurate and valid, as this information is used to produce vital event certificates. Event registrars play an important role in achieving this objective. They are responsible for certifying the accuracy of vital events occurrences and forwarding this information to the Agency.

In this section, we identified the following with regard to protecting the integrity of vital events information:

- 2.1 Processes to ensure accuracy of events registry need improvement.
- 2.2 Controls in place to ensure complete and accurate certificates issued.

2.1 Processes to ensure accuracy of events registry need improvement

Vital events are registered with the assistance of event registrars who certify occurrences of vital events. Historically, designated staff from institutions such as hospitals and funeral homes have acted as event registrars. Additionally individuals such as midwives have also performed the duties of event registrars.

We found:

- Event registrars' appointment documents not in place.
- Complete list of event registrars not maintained and event registrars not validated at event registration.
- Delays noted in registering some vital events.
- Deaths not consistently linked to births.
- No training provided to events registrars.

2.2 Controls in place to ensure complete and accurate certificates issued

We found that the Agency had controls in place to ensure that the vital events certificates issued contained the same information as in the events registry. For example, the Agency staff verified the information customers filled in "Application for a Manitoba Birth Document" in order to obtain new

certificates, and then compared the information on the application to what the Agency had on file prior to issuing a certificate.

On testing a sample of certificates issued we found that the information noted in certificates issued matched with the events registry information. However, the certificates' information is dependent on the information in the registry. As we noted in **SECTION 2.1**, the Agency needs to improve processes to ensure that events registry information is accurate.

3 Certain policies, procedures and guidelines needed to be documented, or reviewed and updated

Policy instruments (policies, procedures, standards and guidelines) play an important role by defining the organization's guiding principles, providing detailed task instructions, and forming the basic structure of business operations. Procedures are designed following the framework of the governing policies. Policy instruments at the Agency support:

- Standardizing the steps followed for event registration — staff members are guided on how to register and amend vital events.
- Minimizing time spent processing registrations.
- Helping staff understand individual and team responsibilities.
- Allowing managers in exercising control by exception.
- Improving information accuracy.
- Protecting the vital events information.

We found:

- Gaps in the development of policy instruments.
- Existing policy instruments not reviewed and updated.

This page is intentionally left blank.

Response from officials

We requested a response from the officials of the Department of Finance. They provided a summary, which is included below.

The Department of Finance is pleased to have this opportunity to respond to the Independent Auditor's Report. We would like to thank the Auditor General (OAG) for its review and recommendations. The scope of the audit and the detail provided will assist in informing current and ongoing efforts to ensure that civil registration in Manitoba is efficient, and that personal and sensitive information about Manitobans is well protected.

The Vital Statistics Agency is a Special Operating Agency that provides civil registration and vital statistics. Civil registration involves continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to Manitoba's population in the provincial vital event registry in accordance with *The Vital Statistics Act*, *The Change of Name Act* and *The Marriage Act*.

In compliance with legislation, the Vital Statistics Agency uses the information registered in the provincial vital event registry to provide evidence of foundational identity or vital status, as well as Manitoba-specific vital event data – enabling individuals to access benefits or study socio-health outcomes.

While digitization efforts were underway prior to the onset of the global COVID-19 pandemic, the Vital Statistics Agency's ability to provide contactless service confirmed the importance of prioritizing transformation and modernization efforts aimed at digitizing operations. For example, upon registration of a birth, families can utilize the birth registration process to seamlessly apply for child benefits and their child's social insurance number without having to attend separate offices in person. In addition, the Vital Statistics Agency experienced a surge in demand for volume and cause of death data, highlighting an area strongly amenable to digitization.

As a critical service provider, the Vital Statistics Agency began ongoing transformation initiatives to modernize its operations and service delivery prior to the delivery of the OAG's report. Examples include the introduction of a weekend staffing pilot in May 2019, and online submission of applications for select documents in October 2019.

In response to COVID-19, the Vital Statistics Agency enhanced operations to prioritize registration activity, essential in enabling access to evidence of foundational identity and vital status (preferably digitally) in order to facilitate access to benefits/programs/supports, as well access to regionally specific data that can inform policy or other decisions. Following prioritization, registration service times for

birth reduced from 12 weeks in February 2019 to 3-4 weeks, and death from 11 weeks in February 2019 to 2-3 weeks.

Prior to receiving this report, the Vital Statistics Agency had already identified and initiated steps to address a number of the recommendations contained in this report. This includes:

- Taking steps to improve physical protection of documents and office premises;
- Enhancing information security, including implementing a process to review access rights on a regular basis, disabling shared accounts and assigning unique IDs to users;
- Exploring options to enter into information sharing agreements with all parties and disseminating vital events documents using registered mail or other secure delivery services;
- Implementing changes to controls that ensure information integrity, including provision of letters to event registrars upon appointment that detail duties and responsibilities legislated in *The Vital Statistics Act*;
- Initiating a review and expansion of policy instruments;

Combined with lessons learned during the COVID-19 pandemic, this report will inform the future modernization efforts of the Vital Statistics Agency, especially in control improvements, management of security and privacy risks, and integrity of registration. Many of the recommendations are reflective of sector-wide security enhancements, and as such, future initiatives by the Vital Statistics Agency will be balanced against the perspective of broader demands in civil registration and vital statistics, as well as funding capacity.

The Department of Finance accepts the findings detailed in the OAG report; we will review how these recommendations will be implemented, and develop and monitor plans of action where needed.

While some recommendations have been addressed, or addressed in part, the Vital Statistics Agency will strive to address all 19 recommendations, with the goal of determining the ability to address recommendations 1, 3-9, 11, 15, and 17 in the short term; followed by recommendations 2, 10, 14 in the medium term; and recommendations 12-13, 16, 18-19 over the long term.

In recognition of the sensitive nature of the work conducted by the Vital Statistics Agency, the Office of the Auditor General provided an internal letter detailing sensitive findings and recommendations. The Vital Statistics Agency responded with a detailed reply that outlined actions already taken, and timelines to address outstanding items.

Background

The Vital Statistics Agency (the Agency) is a Special Operating Agency within the Department of Finance (transferred from the Department of Justice in November 2019) responsible for administering and enforcing *The Vital Statistics Act*.

The primary function of the Agency is to register vital events and provide documents as proof of those events, including foundational identity documents such as birth certificates. Vital events include births, deaths, marriages, stillbirths and name changes. The Agency's database contains vital event records from 1882 to present, which it holds in perpetuity.

As a Special Operating Agency, the Agency is responsible for managing its own information technology needs. The Agency utilizes the government's shared information technology (IT) service provider, Business Transformation and Technology, to provide services such as IT policies and standards, and IT infrastructure.

Since January 1, 1998, the Agency has registered all vital events electronically using a proprietary registry software. Prior to 1998, it recorded vital events using a paper-based system. As part of this changeover, the Agency also transferred historic vital events information into the registry, which now includes nearly 4 million records.

Because of the personal and health information the Agency maintains, it is subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA), and the *Personal Health Information Act* (PHIA), which require public bodies to protect information against risks of unauthorized access, use, disclosure or destruction.

The information maintained by the Agency can be accessed by a variety of individuals. For example, a person whose birth is registered with the Agency can request a copy of their birth certificate. The Agency also shares information with various organizations across the country, including:

- Provincial vital statistics agencies
- Federal and provincial government departments
- Crown corporations
- Health institutions

Since 2019, the Agency has allowed eligible applicants to apply online for birth, death or marriage certificates for events registered in Manitoba.

At the time of our audit, the Agency had 34 full-time employees including one information technology manager to support its information technology needs. According to the Agency's Annual Reports, vital event registrations, documents issued, actual revenue, and net income for the years 2016 to 2019 were as follows:

Activities performed (number of vital event registrations and documents issued, including related services)				Actual revenue and net income (\$ in thousands)	
Year	Event registrations	Documents issued	Total	Revenue	Net income (Before grants & transfers)
2019	41,978	98,567	140,545	\$3,969	\$416
2018	42,942	103,939	146,881	\$4,025	\$422
2017	42,637	102,804	145,441	\$4,048	\$420
2016	40,286	100,633	140,919	\$3,939	\$317

Office location

The Agency operates out of the A. A. Heaps Building, located at 254 Portage Avenue in Winnipeg. The building was originally constructed as a bank in the early 1900s. The Agency occupies the main floor, most of the second floor and a portion of the basement. The main floor consists of a public reception area, as well as a staff work area. There are offices for senior management on the main and second floors.



A. A. HEAPS BUILDING, 254 PORTAGE AVENUE IN WINNIPEG

Objectives

Our objectives were to determine whether the Vital Statistics Agency (the Agency) was properly managing the:

1. Security and privacy risks associated with vital events information.
2. Integrity of vital events information.

Scope and approach

The audit examined if the Agency had sufficient controls in place to protect vital events information. Based on the risks associated with vital events information we limited our examination of controls relating to registration of births, deaths, adoptions, name changes, and changes of sex designation.

We did not examine other vital events information (marriage, stillbirth, and common-law relationship) in the context of audit Objectives 1 and 2 above.

Evidence gathering techniques included in-person meetings, phone calls, and emails with the Agency management, staff, and stakeholders, as well as process walkthroughs, examination of documents, and sample testing.

We interviewed the then Assistant Deputy Minister of Justice, Agency management and staff, other officials within the provincial government, and event registrars (the Agency stakeholders) as we considered necessary. Subsequently, the Agency was brought under the Department of Finance.

We also obtained and reviewed the Agency's strategy documents, business plans, policies and procedures, annual reports, events registry information, as well as other data and records including information provided by the Agency's stakeholders, and we documented the processes.

Where applicable, we selected samples to test if the Agency had been properly managing the security, privacy and integrity risks associated with vital events. Sample sizes varied based on risk.

Criteria

Objective 1

To determine if the Vital Statistics Agency is properly managing the security and privacy risks associated with vital events information, we used the following criteria:

Criteria	Sources
1.1 The Agency should identify, assess and manage the risks associated with the security and privacy of vital events information.	• COSO^(a) • ISACA^(b) Personally identifiable information Audit / Assurance program • COBIT 5^(c)
1.2 The Agency should have controls in place to protect the privacy of vital events information.	• ISO 27002^(d) • ISACA Personally identifiable information Audit / Assurance program • COBIT 5 • FIPPA^(e)
1.3 The Agency should have physical security controls in place to protect vital events information residing at their premises.	• COSO • ISO 27002 • COBIT 5
1.4 The Agency should ensure that there are effective security controls in place to protect the information contained in the events registry.	• COSO • ISO 27002 • COBIT 5
1.5 The Agency should have controls in place to ensure that vital events information is shared with other parties in a secure manner.	• ISO 27002 • ISACA Personally identifiable information Audit / Assurance program • <i>The Vital Statistics Act</i>

(a) The Committee of Sponsoring Organizations' (COSO) provides thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

(b) ISACA is an independent non-profit association that develops globally accepted best practices in information security, assurance, risk management and governance.

(c) COBIT 5 is a leading framework from ISACA for enterprise governance of information and technology.

(d) ISO 27002 is an information security standard published by the International Organization for Standardization.

(e) The Freedom of Information and Protection of Privacy Act (FIPPA) is a Manitoba law that governs handling of personal information by public agencies in the province.

Objective 2

To determine if the Vital Statistics Agency is properly managing the integrity of vital events information, we used the following criteria:

Criteria	Sources
2.1 The Agency should have controls in place to ensure the accuracy of information recorded in the events registry	• COSO • <i>Vital Statistics Act</i> and regulations • ISO 27002
2.2 The Agency should have controls in place to ensure that certificates issued are both complete and accurate.	• COSO • <i>The Vital Statistics Act</i>

This page is intentionally left blank.

1 Weak identification and management of security and privacy risks

The Vital Statistics Agency (the Agency) holds a significant amount of personal information about Manitobans. There is a risk that the confidentiality and privacy of this information could be compromised, therefore, protecting the information from unauthorized access is critical. To determine if the Agency was properly managing the risks associated with the information, we looked at its processes related to vital events registration, information sharing, and certificates issuance. We then assessed whether the Agency had implemented effective controls to mitigate the significant risks.

In this section, we identified the following concerns with regard to protecting the confidentiality and privacy of vital events information:

- No comprehensive risk management processes (**SECTION 1.1**).
- Privacy impact assessments not conducted (**SECTION 1.2**).
- Inadequate physical protection of documents and office premises (**SECTION 1.3**).
- Weak information security controls (**SECTION 1.4**).
- Weak processes for sharing information with other government organizations and individuals (**SECTION 1.5**).

1.1 No comprehensive risk management processes

Failure to identify and assess security and privacy risks could lead to:

- Disclosure of sensitive information.
- Identity theft.
- Negative publicity and reputational damage.
- Loss of public confidence, potential lawsuits, fines and penalties.
- Loss of system use.

A risk assessment identifies events that could cause harm to an organization, how likely those events are to happen, and the potential impacts of the events. With this information, management can decide what controls are necessary to mitigate those risks.

The Agency identified certain risks in its annual business plans, and also submitted a business impact analysis document to the government detailing risks if its services were interrupted for a specified period. Additionally, in 2013-14, the Protective Services Branch conducted a physical security review of the Agency's office to assess physical security risks.

However, we found the Agency did not conduct a comprehensive risk assessment of its environment, nor did it implement regular risk management processes. A comprehensive risk assessment would identify and document all risks, including those related to information security and privacy. Additionally, it would include an assessment of the identified risks to determine their impact and probability of occurrence, as well as commensurate controls to mitigate those risks.

We also observed that in 2018, Archives Manitoba published the "Records and Information Management Framework" for information management in Manitoba. This framework is applicable to all Manitoba government bodies. Archives Manitoba is developing an implementation guide to support departments and agencies in meeting the requirements of the framework. Requirements of the framework include an organization must:

- Identify the records and information needed to support the business.
- Identify, assess the risk, resolve or mitigate, and document any exceptions that affect the creation, integrity, accessibility and usability of its records and information.



Recommendation 1

We recommend that the Vital Statistics Agency conduct a comprehensive risk assessment on its environment to identify and assess the risks associated with vital events information, and subsequently implement controls to mitigate significant risks.

1.2 Privacy impact assessments not conducted

The Agency maintains a significant amount of personal information about Manitobans, including information on births, deaths, adoptions, and changes in sex designation. Protecting this personal information from unauthorized access and disclosure is critical and required by the *Freedom of Information and Protection of Privacy Act*. A privacy breach would affect both the Agency and the individuals whose information is compromised. The Agency's reputation could be damaged and it may face financial and legal implications. An individual whose vital information is compromised may experience physical safety risks, identity theft, loss of business or employment opportunities, and damage to reputation or relationships.

To determine if the Agency was sufficiently managing its privacy risks we looked at whether the Agency was conducting privacy impact assessments.

Privacy impact assessments (PIAs) are a method to identify prospective privacy problems, enable management to implement necessary safeguards early, and provide evidence that the organization considered potential privacy risks. If privacy safeguards are not considered when implementing changes to services or processes, there is a potential that information privacy may be compromised.

We found no evidence of the Agency completing privacy impact assessments relating to the vital events information it manages. Additionally, the Agency did not complete PIAs when new information handling responsibilities were delegated to it (for example, when recently enacted pieces of legislation permitted the opening of pre-adoption records and permitted the removal of the requirement for surgery to change sex designation).

Privacy impact assessment (PIA)

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Source: National Institute of Standards and Technology



Recommendation 2

We recommend that the Vital Statistics Agency conduct privacy impact assessments on its events registry information, and on significant changes to the Agency services or processes, and institute safeguards as needed.

1.3 Inadequate physical protection of documents and office premises

Physical security controls are designed to prevent unauthorized access and to protect personnel from harm, and property from damage. Insufficient or poorly designed and implemented physical security controls diminish the ability to protect personal information and vital event certificates. Physical security controls include perimeter walls, door locks, and surveillance systems. Environmental controls include smoke, fire and heat detection and suppression systems, and uninterruptable power supply.

To determine if the Agency was sufficiently managing the risks associated with physical security, we looked at:

- Physical security policies and procedures.
- Controls implemented to protect physical assets and employees.
- Vital event certificates management.
- The overall physical security environment including perimeter security and the separation of the staff work area from the public area.

In examining the Agency's physical security controls, we found:

- Weak physical security and inventory management controls (**SECTION 1.3.1**).
- Perimeter control weaknesses (**SECTION 1.3.2**).
- Lack of fire suppression controls (**SECTION 1.3.3**).

1.3.1 Weak physical security and inventory management controls

We assessed whether the Agency had implemented sufficient controls to protect physical assets, employees, and vital event certificates and found several weaknesses. Due to sensitive nature of the findings, we presented our detailed findings and recommendations to the Agency's management in an internal letter.



Recommendation 3

We recommend that the Vital Statistics Agency promptly implement the physical controls recommendations presented in our letter to management.

1.3.2 Perimeter control weaknesses

Perimeter controls are an important component of physical security. These controls limit access at the outer boundary of an organization's office space, and provide alerts when security is potentially compromised. Perimeter controls include walls and locked doors. Weak perimeter controls can expose the Agency to theft and damage.

We looked at whether the perimeter controls at the Agency were sufficient to protect the organization and found the following weaknesses and concerns:

- **Access controls to the Agency work area needed improvement**

The work area was not adequately separated from the public area.

- The heights of counters and gates separating the public and work areas were not high enough to prevent unauthorized access to the work area.
- Clients who use a ramp at the main entrance of the Agency's office must pass through the main work area to get to the public reception counters. We observed these clients being escorted by Agency staff.

- **Funeral Board staff had unnecessary access to the Agency work area**

The Funeral Board of Manitoba office is located at second floor of the Agency's building. It had 2 staff members. These staff members must pass through the Agency's work area to get to their offices and to use printers and the lunchroom.



Recommendation 4

We recommend that the Vital Statistics Agency adequately separate the work area from the public area, and restrict access to the agency work area to only authorized Agency staff.

1.3.3 Lack of fire suppression controls

Fire suppression equipment and regular fire inspections are important to protect organizational assets and employees. Regular fire inspections help detect potential fire hazards, and assess the adequacy of fire prevention and detection systems and controls.

We observed:

- There were no water sprinkler systems installed at the Agency office to guard against loss of data and documents.
- Fire inspections were not conducted regularly, the last one was conducted in May 2019 and the one before that in August 2012.



Recommendation 5

We recommend that the Vital Statistics Agency work with Accommodation services to:

- Determine and install the fire suppression mechanism that adequately protects the employees, information and assets, and
- Organize regular fire inspections.

1.4 Weak information security controls

Information security is the protection of organizational information and information systems against unauthorized access or modification. Information security controls protect confidentiality, integrity and availability of computer system data.

The internet enables organizations and individuals to connect to information systems around the world. While this connectivity is a key enabler for organizational success, it also creates an avenue for cyber-hackers to gain unauthorized access to information systems. A determined hacker with the necessary skills, knowledge, and time can compromise computer systems and steal data from anywhere in the world. Numerous information security incidents related to viruses, worms, and other malicious software that compromise information systems occur daily worldwide and the frequency is only increasing. No organization, big or small, public sector or private, is completely safe from cyber threats.

As the Agency maintains a significant amount of personal information on its computer systems from vital events registrations dating back to 1882, it is potentially exposed to several information technology risks, including:

- *Access and privacy risk*—the risk that confidential personal vital events information may be disclosed to, or accessed by, unauthorized individuals. An aspect of this risk is privacy, which is a regulatory requirement to protect personal data and information.
- *Integrity risk*—the risk that the vital events information or data may not be reliable because they are unauthorized, incomplete or inaccurate.

Information security controls help protect the confidentiality, integrity and availability of information. To determine if the Agency had implemented sufficient controls to protect against information security risks we reviewed the Agency processes and practices including the following:

- Performed a process walk through of different vital events registrations (for example, birth and death event registration processes).
- Reviewed registry software access, segregation of duties, and change management controls.
- Identified and tested related automated controls in the registry software.

In examining the Agency's information security controls, we found the following:

- No periodic reviews of users' access rights (**SECTION 1.4.1**).
- Registry software was not configured to segregate some conflicting roles and responsibilities (**SECTION 1.4.2**).
- Privileged users' activities were not monitored (**SECTION 1.4.3**).
- Shared accounts used (**SECTION 1.4.4**).
- Information not classified by level of sensitivity or importance (**SECTION 1.4.5**).
- Some sensitive weaknesses in information security controls (**SECTION 1.4.6**).

1.4.1 No periodic reviews of users' access rights

Information systems users are provided access based on their job requirements. Access rights require adjustment when staff leave, and when users change their roles. Periodically reviewing users' access rights, and withdrawing unneeded access, ensures users' access to organizational systems is appropriately restricted to what they need to perform their jobs. This prevents unauthorized changes to the systems. The provincial government policy and access control standard, established by Business Transformation and Technology (BTT), requires departments — including the Agency — to review access on a periodic basis so that users' access to systems remains appropriate.

Business Transformation and Technology (BTT) is a shared services centre the provincial government established for supporting Information Communication Technology (ICT) assets and developing related internal processes and procedures.

BTT established Manitoba the Access Control Standard for controlling access to Manitoba Information and Communications Technology (ICT) assets. The standard is designed to restrict access to authorized individuals.

Registry software is the electronic application that the Agency uses for registering and maintaining vital events for Manitobans.

We observed the Agency did not have a periodic access rights review process to confirm that users' access rights to the registry software were appropriate. Two out of five users tested had inappropriate access to the registry. One user retained access for over two years after departing from the organization, while another user had access that did not align with the user's job responsibilities.



Recommendation 6

We recommend that the Vital Statistics Agency implement a process to review users' access rights on a regular basis.

1.4.2 Registry software was not configured to segregate some conflicting roles and responsibilities

Segregation of duties is an internal control tool used by organizations to prevent fraud and error. It ensures a single person does not handle all aspects of a transaction, from initiation to completion.

We observed the registry software was not configured to segregate some conflicting user roles and responsibilities, resulting in opportunities for one person to complete a transaction. A segregation of duties conflict we found was some users were able to record and edit vital events registrations and issue vital events certificates (for example, edit birth registration records and issue birth certificates).

In addition, the Agency did not configure registry software to restrict a single user from performing first and second keying of information. As a result, a single person could complete an entire registration without any checks.

Reviews were also not performed of cases where a user both recorded or edited a registration, and issued a vital event certificate, or where the same person did both first and second keying. Without reviews of these events, there is a risk of incorrect, invalid or fictitious information being entered into the registry without being detected, and vital event certificates issued.

First and second keying

The Agency established a process such that one person enters vital events registration information into registry software. This is known as first keying. Subsequently another person re-inputs certain information from the registration form which has already been entered by the first person to validate that the information inputted by the first person is correct. This is known as second keying.



Recommendation 7

We recommend that the Vital Statistics Agency configure the registry software to restrict and segregate users' access such that no single user is able to complete a transaction from beginning to end. Where segregation of duties is not possible, the Agency should monitor the activities of users performing conflicting roles.

1.4.3 Privileged users' activities were not monitored

Privileged users are those users that have elevated privileges (such as administrator rights), giving them significant access to computer systems, including security-relevant functions that ordinary users are not authorized to perform. Because these users have elevated access, there is a greater potential for damage if they misuse their privileges. Additionally, hackers may target privileged users' accounts with the intention of gaining unrestricted system access. The Agency has many privileged users to help support and administer its computer systems that includes Agency, and vendor information technology support staff.

The provincial access control standard requires that additional controls be applied to users with privileged access. These controls can include additional audit logging where possible and reviewing the use of privileged access. We found the Agency did not monitor privileged users' activities to detect unauthorized or suspicious activities for investigation.



Recommendation 8

We recommend that the Vital Statistics Agency monitor privileged users' activities and investigate unauthorized or suspicious activities.

1.4.4 Shared accounts used

The provincial access control standard states: "Users must be subject to a sign-on process that requires identification using unique user IDs." We found some user IDs used by multiple people on the registry software. These user IDs are referred to as shared accounts. As a result, the activities of these accounts cannot be attributed to a specific person, preventing accountability.



Recommendation 9

We recommend that the Vital Statistics Agency disable all shared accounts and assign unique IDs to each user.

1.4.5 Information not classified by level of sensitivity or importance

Not all information an organization holds is of equal importance and sensitivity. Information classification is a critical part of information management, and helps apply commensurate controls for protecting the information of different sensitivity categories. For example, for the highest sensitivity category the strictest controls should be applied, while for public information there may be no or minimal controls applied. In addition to defining the controls to be applied to different sensitivity categories, information classification also helps those involved with information handling take necessary precautions and apply the required controls to protect the information from unauthorized use and disclosure.

Provincial data classification guidelines provide examples of handling and security measures for different information classification levels (restricted, protected and public).

We found the Agency had not classified its information based on the sensitivity of the information. In absence of information classification there is a risk that:

- The information may not be protected matching its sensitivity levels.
- Similar protection controls may be applied to all information resources irrespective of the sensitivity levels, which may lead to over or under protection. This may result in inefficient use of resources, and potentially security breaches.



Recommendation 10

We recommend that the Vital Statistics Agency classify its information resources in different information categories depending on sensitivity, and upon classification define and apply controls to those categories based on established data classification guidelines.

1.4.6 Some sensitive weaknesses in information security controls

Information security controls help protect the confidentiality, integrity and availability of information and include both preventative and detective controls. Insufficient or poorly designed and implemented information security controls diminish the ability to protect information and information systems. We assessed whether the Agency had implemented sufficient controls to protect its systems. While the Agency had many information security controls, we found several weaknesses. Due to sensitive nature of the security findings, we presented our detailed findings and recommendations to the Agency's management in an internal letter.



Recommendation 11

We recommend that the Vital Statistics Agency promptly implement the security control recommendations presented in our letter to management.

1.5 Weak processes for sharing information with other government organizations and individuals

The Agency shares vital events information with various federal and provincial government departments and provincial vital statistics agencies. Information is shared with those organizations for purposes such as:

- Policy development.
- Confirming eligibility for public programs and benefits.
- Reporting out-of-province deaths.

As per section 12(1) of the Vital Statistics Agency regulations, subject to certain conditions duly authorized representatives of federal or provincial governments in the course of and for the purpose of discharging their official duties may have access to, or receive copies of or information from, the records in the office of the director (of Vital Statistics Agency) or of an event registrar.

The Agency also shares vital events information with authorized individuals. For example, a person whose birth is registered with the Agency can request a copy of their birth certificate.

It is important to sufficiently protect personal information from inappropriate access and disclosure.

In examining the Agency's information sharing processes, we found:

- Mutual information sharing responsibilities not always defined (**SECTION 1.5.1**).
- Secure mail not always used for delivering certificates and registration forms (**SECTION 1.5.2**).

1.5.1 Mutual information sharing responsibilities not always defined

We found the Agency did not enter into information sharing agreements with 5 of 11 organizations it shared information with. These organizations include other provincial vital statistics organizations. Without agreements, it is unclear what each organizations' responsibilities are regarding information protection.

In addition to stipulating each parties' roles and responsibilities regarding information protection, information sharing agreements, also should specify:

- The nature, contents, format and frequency of the information that can be shared.
- Information encryption requirements.
- Media to be used for information sharing.
- Retention period of the information shared.
- The Agency's right to an audit of the organizations it shares information with including security measures, data handling, access control, and physical security.



Recommendation 12

We recommend that the Vital Statistics Agency enter into information sharing agreements with all the parties it shares information.

1.5.2. Secure mail not always used for delivering certificates and registration forms.

The Agency uses regular mail delivery services to send vital events certificates, except when applicants elect to pay for rushed issuance. Regular mail services are also used to deliver vital events registration forms to the Agency by all but three events registrars out of 20 registrars we visited. These three use secure medical courier services.

When using regular mail, there is a risk that vital events certificates and vital events registration information may be delivered to unintended parties or lost in transit, and therefore may result in a breach of an individual's privacy, identity theft and fraud.

Event registrars

Under s.27(1) of *The Vital Statistics Act*, the Agency director may appoint a person to be an event registrar with respect to one or more of the following registrations under the Act:

- births
- marriages
- deaths
- stillbirths



Recommendation 13

We recommend that the Vital Statistics Agency deliver and receive vital events documents and confidential or personal information using registered mail or other secure delivery services.

2 Weaknesses in the controls that ensure information integrity

It is important to ensure that the Agency's events registry is complete, accurate and valid, as this information is used to produce vital event certificates. Event registrars play an important role in achieving this objective. They are responsible for certifying the accuracy of vital events occurrences and forwarding this information to the Agency.

In this section, we identified the following issues with regard to protecting the integrity of vital events information.

- Processes to ensure accuracy of events registry need improvement (**SECTION 2.1**).
- Controls in place to ensure complete and accurate certificates issued (**SECTION 2.2**).

2.1 Processes to ensure accuracy of events registry need improvement

Vital events are registered with the assistance of event registrars who certify occurrences of vital events. Historically, designated staff from institutions such as hospitals and funeral homes have acted as event registrars. Additionally individuals such as midwives have also performed the duties of event registrars.

When a birth occurs, event registrars provide a vital event registration form to the parents. The parents fill in information including the mother's name, her birth date, place of birth and address. The mother's social insurance number is also required if the parents elect to apply to the Canada Revenue Agency for Canada child benefits. The event registrars' staff then certify the event occurrence by signing the registration form and adding the unique identification number of the birth facility. The birth facility could be a hospital, a birth station or a midwifery location. The event registrar forwards the completed registration forms to the Agency for registration.

In case of a death that occurs in Manitoba, a two-page registration-of-death form is completed. On the first page the funeral director ensures completion of all personal particulars of the deceased, signs the event registrar certification and forwards it to the Agency. On the second page, the attending physician certifies cause-of-the-death and then provides the form to the health institutions' event registrar to sign the certification and forward it to the Agency.

After the Agency receives a registration form it becomes a permanent legal record. Changes cannot be made easily. Correcting errors or adding missing information can only be done when permitted by law. The applicant may be charged fees for making changes.

In examining the Agency's events registration processes, we identified the following concerns:

- Event registrars' appointment documents not in place (**SECTION 2.1.1**).
- Complete list of event registrars not maintained and event registrars not validated at event registration (**SECTION 2.1.2**).
- Delays noted in registering some vital events (**SECTION 2.1.3**).

- Deaths not consistently linked to births (SECTION 2.1.4).
- No training provided to events registrars (SECTION 2.1.5).

2.1.1 Event registrars' appointment documents not in place

Section 27 (1) of *The Vital Statistics Act* allows the Agency's director to appoint a person to be an event registrar to register births, marriages, deaths, and stillbirths.

We confirmed with Agency management that they did not have event registrars' appointment documents in place for 5 years prior to October 23, 2018. Since that date, individuals that were newly appointed as event registrars were provided with letters describing their responsibilities as prescribed by *The Vital Statistics Act*.



Recommendation 14

We recommend that the Vital Statistics Agency issue appointment letters to all event registrars which would detail their duties and responsibilities in accordance with *The Vital Statistics Act* and that the appointment letters include a sign off by the registrars acknowledging their responsibilities.

2.1.2 Complete list of event registrars not maintained and event registrars not validated at event registration

The Agency maintains information on event registrars in its registry software. This includes the unique identification number of the event registrar organization (hospital, funeral home, etc.), and names of the staff serving as event registrars. Event registrars certify event occurrences by signing their name and writing their organization's unique identification number on registration forms, and then forwarding those forms to the Agency. The Agency's staff members are required to validate the event registrar by matching the organization's unique number and names of the individuals who certified the registration, to the information maintained in the registry software.

We found the list of event registrars maintained by the Agency did not include midwives who certified birth registration forms and all the individuals who certified death registration forms. Upon further inquiry, the Agency confirmed it did not include the following event registrars in its list:

Midwives are health professionals who provide primary care to women and their babies during pregnancy, labour, birth and the postpartum period. Like other events registrars, midwives are required to send birth registration forms to the Agency for the births they assist with.

- midwives
- doctors who help plan home-deaths
- medical examiners who determine the causes of deaths
- a complete and accurate list of staff serving as event registrars for organizations such as hospitals and funeral homes.

We reviewed a sample of 30 births and 20 death registration forms. In the sample, we found:

- No evidence to support that the Agency's staff members had validated the individuals who certified the registrations before inputting the information into the events registry.
- Some death registration forms were certified by persons not on the Agency's list.
- No further information was obtained to validate the birth registrations submitted by midwives. As the Agency cannot validate the event registrars not maintained in their list, other information is necessary to confirm the event occurrence. An example other information could be postnatal medical examination records in case of birth events.

As a result, there is a potential that invalid or inaccurate vital events may be registered.



Recommendation 15

We recommend that the Vital Statistics Agency:

- Maintain a complete list of event registrars, including midwives, and
- Validate the events registrar organizations' unique number and the certifying individuals' names before inputting the information into the events registry. In cases where the event registrars cannot be validated, the Agency should obtain other information to confirm the occurrence of the vital event.

2.1.3 Delays noted in registering some vital events

We tested a sample of 30 birth registrations from 2015 to 2017 and found:

- 15 (50%) were registered within 4 weeks of their receipt at the Agency,
- 8 (27%) were registered 4 - 6 weeks of their receipt,
- 2 (7%) took 9 weeks to be registered, and
- The remaining 5 were registered in excess of 10 weeks while the Agency waited for additional information from the parents.

We also looked at the Agency's more recent daily processing information for October 26, 2018 which indicated that both birth and death registrations were pending registration after 8 weeks. This information confirms that events' registration times vary.

Delays in birth and death registrations can have significant impacts. For example, parents cannot obtain a social insurance number, health card or passport for their child, or receive child welfare benefits, until a birth has been registered. Delays in death registrations affect linking deaths to Manitoba birth records as well as in death certificates issuances. As a result, there will be delays in settling inheritance claims regarding property transfer for a deceased's estate.

The Agency management identified that delays related to factors such as staff shortages and increased volumes of marriage registrations during the summer.



Recommendation 16

We recommend that the Vital Statistics Agency implement methods to expedite processing times for vital events' registrations.

2.1.4 Deaths not consistently linked to births

Best practices recommend that all in-province, out-of-province, and out-of-country death and birth registrations should be cross-matched where such data is available, to decrease the risk of identity theft.

Using obituary information, individuals may obtain a deceased person's birth certificate for the purpose of committing fraud. These individuals take advantage of the fact that not all birth and death records are linked, or linked in a timely manner.

We assessed whether the Agency implemented sufficient controls for linking deaths to Manitoba births, and we found weaknesses. Due to sensitive nature of these findings, we presented our detailed findings and recommendations to the Agency's management in an internal letter.



Recommendation 17

We recommend that the Vital Statistics Agency promptly implement the control recommendations for linking deaths to births presented in our letter to management.

2.1.5 No training provided to events registrars

The Agency did not train event registrars on how to prepare, compile and forward vital events information, or how to maintain the privacy and security of vital events information. It is essential that vital events registrars provide complete, accurate and valid information to the Agency, and that they understand their responsibility for maintaining its security and privacy.

The Vital Statistics Act has prescribed time limits within which vital events registration forms must be forwarded to the Agency by the events registrars. However, at one of the midwifery locations we visited, the midwife was not aware of the timeframe within which the birth registration forms were to be submitted to the Agency. During our visits to the events registrars, we also found some were not aware of the Statutory Declaration of a Married Woman. Additionally, the declaration forms were not available to the events registrars.

Statutory declaration of a married woman under section 3(7)(b) of the *Vital Statistics Act* is a document that a married woman files with the Agency's director declaring that at the time of conception of her child she was living separate and apart from her husband and that her husband is not the father of the child.

Further, in April 2017, the Agency introduced new birth registration forms without providing any training to the events registrars on what changed from the previous version.

Training for events registrars would help to ensure they are aware of their responsibilities that support accurate and timely event registration. Additionally, without training regarding the safe and secure handling of registration information there is a risk of privacy breach.



Recommendation 18

We recommend that the Vital Statistics Agency periodically train the events registrars, for example:

- In vital events registration information creation, compilation and forwarding processes.
- In maintaining privacy and security of the clients' information.
- When introducing new forms and significant changes in processes.

2.2 Controls in place to ensure complete and accurate certificates issued

We found that the Agency had controls in place to ensure that the vital events certificates issued contained the same information as in the events registry. For example, the Agency staff verified the information customers filled in "Application for a Manitoba Birth Document" in order to obtain new certificates, and then compared the information on the application to what the Agency had on file prior to issuing a certificate.

On testing a sample of certificates issued we found that the information noted in certificates issued matched with the events registry information. However, the certificates' information is dependent on the information in the registry. As we noted in **SECTION 2.1**, the Agency needs to improve processes to ensure that events registry information is accurate.

3 Certain policies, procedures and guidelines needed to be documented, or reviewed and updated

Policy instruments (policies, procedures, standards and guidelines) play an important role by defining the organization's guiding principles, providing detailed task instructions, and forming the basic structure of business operations. Procedures are designed following the framework of the governing policies. Policy instruments at the Agency support:

- Standardizing the steps to be followed for events registration — staff members are guided how to register and amend vital events.
- Minimizing time spent processing registrations.
- Helping staff understand individual and team responsibilities.
- Allowing managers to exercise control by exception.
- Improving information accuracy.
- Protecting the vital events information.

Policy instruments also provide clarity to the staff when dealing with accountability issues and activities that are of critical importance to the organization and the information in its custody such as, privacy and information security, health and safety, legal liabilities and, regulatory requirements.

In examining the Agency's policy instruments, we found:

- Gaps in the development of policy instruments (**SECTION 3.1**).
- Existing policy instruments not reviewed and updated (**SECTION 3.2**).

3.1 Gaps in the development of policy instruments

We found policy instruments were not developed in many cases to provide staff with guidance on how to perform regular activities in a standard and repeatable manner. Policy instruments had not been developed in the following instances:

- **Vital events registration** – to register, process and amend vital events in the events registry by the Agency staff or for the events registrars' activities ensuring information is received accurately, completely and timely.
- **Vital events certificates** – to issue accurate certificates to appropriate individuals, and for certificate inventory management.
- **Access controls** – in regards to activities for provisioning access to the registry software and performing users' access rights reviews. Provincial standards require processes for authorizing users must be defined in writing.

- **Data classification** – to provide staff with roles and responsibilities in regard to classifying and handling data in different circumstances such as data at-rest, in-transit and information sharing practices.
- **Physical security and Privacy Protection** – as comprehensive policy instruments covering activities such as identifying the information to be protected, the appropriate level of physical protection to apply based on the information and maintaining and periodically testing of physical security equipment (i.e. alarms, cameras, etc.).

3.2 Existing policy instruments not reviewed and updated

Regularly reviewing policy instruments keeps organizations up to date with regulations, technology, and best practices. Policy reviews ensure that the policies are consistent and effective. Outdated policy instruments can leave organizations at risk, as old policies may fail to comply with new regulations and processes, or may not address new systems or technology, which can result in inconsistent practices.

A review of the Agency's policies showed none had been updated since implementation. Further, the policies did not indicate any date by which they should be reviewed. For example, there was no revision date indicated or time frame stated within which the following policies should be reviewed:

- Non-VSA Employee Visitors (2012-10-15) and
- Employee Orientation (2014-04-04).

Current "Non-VSA Employee Visitors policy (2012-10-15)" permitted admitting visiting former employees, friends, family and meeting participants to the boardroom. The boardroom, at the time of our review was being used for housing important Agency documents, however the policy was not revised to reflect the changed situation. Additionally 'Visitors' and Non-VSA Employee Visitors policies had conflicting statements. As per Visitors policy "all visitors must sign in and wear a visitor badge before entering any of the Agency's work areas", whereas "Non-VSA Employee Visitors" policy stated "visitors must never be in secure work areas at any time".



Recommendation 19

We recommend that the Vital Statistics Agency implement, review and update their policy instruments where required.

Conclusion

We concluded that the Agency was not properly managing the:

- Security and privacy risks associated with vital events information.
- Integrity of vital events information.

As a result, control improvements are needed.

This page is intentionally left blank.

Additional information about the audit

This independent assurance report was prepared by the Office of the Auditor General of Manitoba on the Vital Statistics Agency. Our responsibility was to provide objective information, advice and assurance to assist the Legislature in its scrutiny of the government's management of resources and programs, and to conclude on whether the Vital Statistics Agency complies in all significant respects with the applicable criteria.

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard for Assurance Engagements (CSAE) 3001—Direct Engagements set out by the Chartered Professional Accountants of Canada (CPA Canada) in the CPA Canada Handbook — Assurance.

The Office applies Canadian Standard on Quality Control 1 and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we have complied with the independence and other ethical requirements of the Roles of Professional Conduct of Chartered Professional Accountants of Manitoba and the Code of Values, Ethics and Professional Conduct of the Office of the Auditor General of Manitoba. Both the Rules of Professional Conduct and the Code are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

In accordance with our regular audit process, we obtained the following from management:

1. confirmation of management's responsibility for the subject under audit
2. acknowledgement of the suitability of the criteria used in the audit
3. confirmation that all known information that has been requested, or that could affect the findings or audit conclusion, has been provided; and
4. confirmation that the audit report is factually accurate.

Period covered by the audit

The audit covered the period between March 2015 and March 2017. This is the period to which the audit conclusion applies. However, to gain a more complete understanding of the subject matter of the audit, we also examined certain matters prior to and subsequent to the audit coverage period.

Date of the audit report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on July 22, 2020, in Winnipeg, Manitoba.

This page is intentionally left blank.

Summary of recommendations

In this section we provide a summary of the recommendations. The Department of Finance has provided an overall response to our report and recommendations that can be found in the Response from officials section (see page 11).

Section 1: Weak identification and management of security and privacy risks

1. We recommend that the Vital Statistics Agency conduct a comprehensive risk assessment on its environment to identify and assess the risks associated with vital events information, and subsequently implement controls to mitigate significant risks.
2. We recommend that the Vital Statistics Agency conduct privacy impact assessments on its events registry information, and on significant changes to the Agency services or processes, and institute safeguards as needed.
3. We recommend that the Vital Statistics Agency promptly implement the physical controls recommendations presented in our letter to management.
4. We recommend that the Vital Statistics Agency adequately separate the work area from the public area, and restrict access to the agency work area to only authorized Agency staff.
5. We recommend that the Vital Statistics Agency work with Accommodation services to:
 - Determine and install the fire suppression mechanism that adequately protects the employees, information and assets, and
 - Organize regular fire inspections.
6. We recommend that the Vital Statistics Agency implement a process to review users' access rights on a regular basis.
7. We recommend that the Vital Statistics Agency configure the registry software to restrict and segregate users' access such that no single user is able to complete a transaction from beginning to end. Where segregation of duties is not possible, the Agency should monitor the activities of users performing conflicting roles.
8. We recommend that the Vital Statistics Agency monitor privileged users' activities and investigate unauthorized or suspicious activities.
9. We recommend that the Vital Statistics Agency disable all shared accounts and assign unique IDs to each user.

10. We recommend that the Vital Statistics Agency classify its information resources in different information categories depending on sensitivity, and upon classification define and apply controls to those categories based on established data classification guidelines.
11. We recommend that the Vital Statistics Agency promptly implement the security control recommendations presented in our letter to management.
12. We recommend that the Vital Statistics Agency enter into information sharing agreements with all the parties it shares information.
13. We recommend that the Vital Statistics Agency deliver and receive vital events documents and confidential or personal information using registered mail or other secure delivery services.

Section 2: Weaknesses in the controls that ensure information integrity

14. We recommend that the Agency issue appointment letters to all event registrars which would detail their duties and responsibilities in accordance with the Vital Statistics Act and that the appointment letters include a sign off by the registrars acknowledging their responsibilities.
15. We recommend that the Agency:
 - Maintain a complete list of event registrars, including midwives, and
 - Validate the events registrar organizations' unique number and the certifying individuals' names before inputting the information into the events registry. In cases where the event registrars cannot be validated, the Agency should obtain other information to confirm the occurrence of the vital event.
16. We recommend that the Vital Statistics Agency implement methods to expedite processing times for vital events' registrations.
17. We recommend that the Vital Statistics Agency promptly implement the control recommendations for linking deaths to births presented in our letter to management.
18. We recommend that the Vital Statistics Agency periodically train the events registrars, for example:
 - In vital events registration information creation, compilation and forwarding processes.
 - In maintaining privacy and security of the clients' information.
 - When introducing new forms and significant changes in processes.

Section 3: Certain policies, procedures and guidelines needed to be documented, or reviewed and updated

19. We recommend that the Vital Statistics Agency implement, review and update their policy instruments where required.

» **Our Vision**

Valued for positively influencing public sector performance through impactful audit work and reports.

» **Our Mission**

To focus our attention on areas of strategic importance to the Legislative Assembly, and to provide Members of the Legislative Assembly with reliable and efficient audits.

Our mission includes easy-to-understand audit reports that include discussions of good practices within audited entities, and recommendations that, when implemented, will have a significant impact on the performance of government.

» **Our Values** | Accountability | Integrity | Trust | Collaboration | Innovation | Growth

Auditor General

Tyson Shtykalo

Director, IT Audit, Operations and Security

Wade Bo-Maguire

Principal

Ganesh Sharma

Communications Manager

Frank Landry

Admin Support

Jomay Amora-Dueck

Tara MacKay

Graphic Design

Waterloo Design House



Auditor General
MANITOBA

For more information, please contact our office at:

Office of the Auditor General
500-330 Portage Avenue
Winnipeg, Manitoba R3C 0C4

Phone: 204-945-3790 Fax: 204-945-2169
contact@oag.mb.ca | www.oag.mb.ca

-  [Facebook.com/AuditorGenMB](https://www.facebook.com/AuditorGenMB)
-  [Twitter.com/AuditorGenMB](https://twitter.com/AuditorGenMB)
-  [Linkedin.com/company/manitoba-auditor-general](https://www.linkedin.com/company/manitoba-auditor-general)