



AUDIT REPORT

Health and Social Services

**Environmental Health Inspection
Program**

Operational Audit

October 2015





OCT 23 2015

CONFIDENTIAL

File: 7850-20-HSS-151-138

MS. DEBBIE DELANCEY
DEPUTY MINISTER
HEALTH AND SOCIAL SERVICES

Audit Report: Environmental Health Inspection Program
Audit Period: January 2009 to August 2015

A. SCOPE AND OBJECTIVES

The Audit Committee Chair approved the Department of Health and Social Services (Department) management request for an audit of the Environmental Health Inspection Program managed by the Environmental Health Unit (EH Unit). The audit objectives were to assess the efficiency and effectiveness of the health inspection processes by examining the internal controls for the governance framework, information integrity, compliance and asset safety. We examined health inspection processes for food safety, day care, drinking water and rabies by:

- reviewing relevant legislation, guidelines and policies referenced by the EH Unit
- conducting data analysis of the EH Unit information database
- interviewing the EH Unit's staff
- consulting with Subject Matter Expert (SME).

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.



B. BACKGROUND

In 2009, responsibility for managing potential environmental public health risks to the Northwest Territories (NWT) population was transferred from the Stanton Territorial Hospital to the Department. Stanton's EH Unit that transferred to the Department included a Chief Environmental Health Officer (Chief EHO) and team of Environmental Health Officers (EHOs). These positions continue to have delegated authority under the *Public Health Act* and other relevant legislation to inspect premises such as food establishments, day cares and water treatment plant operations in the NWT.

The Chief EHO currently reported to the Director of Population Health for program administration, and also to the Chief Public Health Officer (CPHO) for delegated responsibilities under the *Public Health Act*. The EH Unit had seven EHOs and one support staff that report to the Chief EHO. EHOs were responsible to carry out the health inspections, investigations and issue orders to protect public health as required under legislation. The Unit's main office was in Yellowknife with three regional offices in Inuvik, Norman Wells and Hay River.

The EH Unit was responsible to inspect 14 mandated Environmental Health Program areas (**Appendix A refers**). EHOs were responsible for a range of duties such as education, awareness work, and participating in environmental regulatory review processes. EHOs primary role was to conduct health inspections. Each EHO was assigned to conduct inspections based on geographic locations in NWT. The assignment or scheduling of inspections were subject to change based on the:

- volume or complexity of inspection activities
- response to urgent complaints received from the public or a disease outbreak
- access to a site or community due to weather conditions, or
- availability of operators.

Out of the 14 inspection areas mandated to EH Unit, four areas constituted the majority of inspections conducted by the EH Unit. According to the EH Unit:

1. The **Food Safety Inspection Program** was authorized under the *NWT Food Establishment Safety Regulations*. The goal of the Food Safety Program was to reduce the number of foodborne illness. The EH Unit issued food establishment permits for any place where food was handled and intended for public consumption. In July 2015, there were over 500 food operators with food establishment permits in the NWT. EHOs used a risk-based assessment process to determine the frequency of the inspections. The high risk facilities were inspected more than once per year. The EH Unit posted the results of private food operator inspections on the Department's website as they were completed.

2. The **Day Care Inspection Program** was authorized under the *Child Day Care Standard Regulations*. The purpose was to set minimum standards that ensure the quality care, instruction and supervision of children. The EHOs inspected child day care facilities at least once per year. In July 2015, there were approximately 200 child day care facilities in NWT. EHOs inspection reports were provided to the Day Care Operators and the Early Childhood Consultants at the Department of Education, Culture and Employment.

3. The **Drinking Water Inspection Program** was authorized under the *Water Supply System Regulations*. EHOs were responsible for regulating the public water supply systems in the NWT. In July 2015, the NWT had over 40 public water supply systems. EHOs ensured the safety of drinking water by monitoring to ensure all water supply systems in NWT were in compliance with the *Water Systems Supply Regulations*. The Department's CPHO recommended solutions for safety issues, reviewed sample reports, advised on the safety of the water for human consumption, and issued boil water advisories/orders. All public complaints were investigated to ensure drinking water safety.

The Department of Municipal and Corporate Affairs published the NWT Drinking Water Quality Database and an Annual GNWT Report on Drinking Water (Annual report) on their website. Environmental public health information was included in the Annual report.

4. The **Rabies Prevention Program** was authorized under the *Public Health Act*. EHOs were responsible to investigate animal bite incidents and implement prevention and control measures. Although there has never been a case of human rabies in the NWT, northern residents living in remote communities face a relatively high risk of exposure to the rabies virus. Animal bite complaints were investigated immediately to ensure public safety given the level of high risk.

The EH Unit followed guidance from the CPHO and Communicable Disease Manual as well as Canadian Food Inspection Agency (CFIA) guidelines to investigate all animal contact incidents and prevent rabies in humans. All suspected rabies cases were reported to the Chief EHO and CPHO. The EH Unit had over 900 animal bite incidents reported over a six-year period (April 2009 to August 2015). EHOs were assigned to investigate the animal bite incident, quarantine the animal or consult the CPHO and report on all investigations.

A number of environmental health inspection standards were available and have been well researched by professional associations, universities and other jurisdictions. The Chief EHO represented the Government of the NWT on national, intergovernmental and interdepartmental committees' including national standard setting committees.

C. OVERVIEW

Responsible governments have been expected to provide services that protect the health of the public. A goal of the 17th NWT Legislative Assembly was of a NWT population living in a healthy environment. The Environmental Health Inspection Program delivered by the Department supported this goal.

There was a high level of inherent risk associated with conducting health inspections over a widely dispersed territory with remote communities that were required to be visited a minimum of two times per year. The logistics of delivering a diverse mandate in 31 communities, where 27 communities were served only with inspection visits, was a challenge. To address this and other operational challenges, the Department required a high level of internal control capacity to match the associated risk.

According to the Director of Population Health, the Department started an inspection review process in 2014-2015 fiscal year to improve internal accountability mechanisms as well as overall efficiency and effectiveness of the EH Unit operations. The foundation of an efficient and effective operation starts with a clear governance framework that includes legislation, regulations, policies, procedures as well as current job descriptions. The development of a governance framework can be enhanced with an accepted globally or nationally recognized public health inspection standard. These standards include best practices which can be used to enhance policies and procedures and allow for continuous improvement in the NWT inspection program.

A well-documented risk-based governance framework supports the sustainability of the inspection program by mitigating the risk of staff turnover and change management issues. The impact of change gets mitigated as the EH Unit staff have the tools to continue using the proven processes that work in the NWT.

Collection of information that was relevant, reliable, complete, accurate and timely for the inspection program would allow management to monitor the operations and make strategic decisions. The database used by the EH Unit to track inspection information required further work.

In response to the audit observations, the Department developed a detailed management action plan to address the governance framework and information integrity risks. By addressing these areas, Department management will be in a better position to manage and monitor the compliance of the EH Unit's inspections with accepted and adopted standards, assess the EH Unit practices for the effective delivery of their mandated programs, increase consistency and transparency of the EH Unit's actions and create an overall efficient and effective program that aids in having the NWT population living in a healthy environment.

D. OBSERVATIONS AND MANAGEMENT ACTION PLANS

Observation 1: Public Health Inspection Standards	1 of 6
<p>The Department did not adopt a globally recognized set of public health inspection standards to support the continuous improvement of the EH Unit.</p>	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ Globally recognized public health inspection framework (standards) could serve as a mechanism for ensuring that an organization's designated officers consistently and accurately provide essential services in a timely, cost-effective manner. ■ <i>Public Health Act</i> (Act) s. 51 stated where a written code or standard has been established, the Commissioner on the recommendation of the Minister may adopt the code in the regulations. ■ During our review of the <i>Food Establishment Safety Regulations, the National Building Code of Canada</i> was the only code specified. ■ Out of the four areas, the EH Unit posted guidelines and codes on their website for three areas: food safety, drinking water and rabies programs. ■ According to the job descriptions, EHOs were required to: <ul style="list-style-type: none"> ○ be certified public health inspectors through the Canadian Institute of Public Health Inspectors ○ provide technical expertise in accordance with professional standards, legislation and evidence based best practice. ■ The Chief EHO stated the EHOs^{14(1)(a)} EHOs used their professional judgment, training, experience and best practices when conducting inspections and completing NWT forms and checklists. ■ The tools used by the EHOs to conduct food establishment risk assessment and the inspection checklists were based on research and past practices. According to the Chief EHO, the checklists were researched and adapted from those in use by other Canadian jurisdictions. ■ There were international and national standards available for public health inspection. For example, Public Health Services Standards from Accreditation Canada has standards for "Protecting the Health of the Population". These standards provided guidelines for the frequency and scheduling of inspections based on risk, responding to requests for information on criteria and results of inspections. 	
<p>Risk:</p> <ul style="list-style-type: none"> ■ Policies and procedures developed by the Department may not reflect current best practices prescribed in an accepted globally recognized set of public health inspection standards. ■ A range of health inspection standards can be used by stakeholders to advocate their agenda where stakeholder expectations do not align with the roles and responsibilities of the Department. 	
<p>Management Action Plan:</p> <ol style="list-style-type: none"> a) Chief EHO, in consultation with a SME, will research public health inspection standards suitable for the NWT and recommend recognized environmental health inspection standards to the CPHO and Director of Population Health for review by November 2016. b) CPHO will approve NWT standards within 3 months of receiving draft standards. It is recognized that standards requiring changes to GNWT regulations may take longer to approve. c) At the time of CPHO approval of standards, the Chief EHO will establish a process to review and update NWT standards in light of globally recognized standards. 	

Observation 2: Public Health Inspection Policies	2 of 6
<p>The Department did not have comprehensive policies on how the EH Unit will protect public health pursuant to the <i>Public Health Act</i>.</p>	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ GNWT policies represent its commitment to the public to follow an action or course of action in pursuit of approved objectives. ■ According to the job description (JD), Chief EHO manages the 16 Inspection Program components mandated by the <i>Public Health Act</i> and <i>Regulations</i>. The Chief EHO also leads the analysis, development and revision of relevant Environmental Health policy and procedures, guidelines and standards. ■ From the four program areas we examined, the Department provided a policy for posting results of the food safety inspections only. A copy of that policy was not available on their website. ■ The "Food Establishment policy on posting of inspection reports, written orders and court actions" stated that inspections on all food establishments will be made public. According to the website, the Department posted the results of all food inspections as they were completed. In practice, only private food establishment inspections were posted on the website. For example, Chief EHO explained that the North Slave Correctional Centre inspections were not posted on the website. If the intent was to publish only private food establishments, this should be stated clearly in the policy. Otherwise it appeared the policy was applied inconsistently and GNWT managed food establishments were exempt from this provision. ■ The Environmental Unit did not have policies on conducting the Drinking Water, Day Care, Rabies and Food Safety inspections. The Chief EHO 14(1)(a) 14(1)(a) ■ Some regulations provided clear direction, for example, <i>Water Supply System Regulation</i> and <i>Child Day Care Standards Regulation</i>. The EH Unit did not have written direction to staff on how to meet those regulatory requirements. 	
<p>Risk:</p> <ul style="list-style-type: none"> ■ A policy vacuum leads to unclear roles and responsibilities of staff, resulting in a lack of accountability and preventing the EH Unit from achieving its program objectives. ■ Department may not have clear understanding of the EH Unit's role in protecting public health and creating a gap in the health of NWT communities. 	
<p>Management Action Plan:</p> <ol style="list-style-type: none"> a) Within 6 months after the standards have been approved (Observation 1), the Chief EHO will use a risk based approach to identify and develop environmental health inspection policies that are aligned with the standards. b) CPHO will approve these policies within 3 months of receiving draft policies. c) At the time of CPHO approval of policies, the Chief EHO will establish a process to review and update policies in line with adopted globally recognized standards. 	

Observation 3: Public Health Inspection Procedures	3 of 6
<p>The EH Unit did not have comprehensive, written procedures to provide clear direction for the EHOs to carry out their inspections consistently and reliably.</p>	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ Procedures provide clear direction to staff on inspection processes that will meet environmental health standards, legislation and policy requirements. ■ The EH Unit had written draft procedures for rental housing complaint investigations, playgrounds for child day cares, handling uninspected wild fish and game, sale of unprocessed fish by fishermen, and animal bite investigations. ■ These procedures did not cover all processes in the four program areas reviewed. ■ The inspection processes in the four program areas were not fully documented but the EH Unit had knowledgeable staff that explained the current inspection processes. ■ Management indicated informal procedures existed and were circulated by the former Chief EHO. This information was no longer accessible or not communicated when there was staff turnover of the Chief EHO. ■ The Chief EHO held weekly meetings with EHOs to give verbal direction and to coordinate and schedule inspections based on the EHOs assigned geographic locations. The Chief EHO would provide advice and guidance on schedules and inspection results upon request or when problems were noted. ■ The tool used by EHOs for risk assessment and inspection checklists did not specify the criteria used to measure compliance. For example, "Adequate equipment to maintain food temperatures" did not clearly explain what adequate equipment meant. ■ The Chief EHO noted that the inspections were not consistent. For example, 14(1)(a) [REDACTED] ■ There were no written procedures on follow up inspections and submission of reports. According to the Chief EHO, the inspection results should be submitted within 5 days after inspection at the latest. 	
<p>Risk:</p> <p>Lack of:</p> <ul style="list-style-type: none"> ■ clear procedures and tools may result in increase in procedural errors. ■ accountability and transparency in the inspection process. ■ continuity in providing inspection services during staff turnover and change management. ■ continuous improvement during staff turnover and change management. 	
<p>Management Action Plan:</p> <ol style="list-style-type: none"> a) Within 6 months after the policies have been approved (Observation 2), the Chief EHO will develop and present to the Director of Population Health and CPHO environmental health inspection procedures that are aligned with the policies (Observation 2). b) CPHO will approve these procedures within 3 months of receiving draft procedures. c) At the time of CPHO approval of procedures, the Chief EHO will establish a process to update procedures on regular basis and a mechanism to document the training and development of EHOs using the updated procedures. 	

Observation 4: Job Descriptions	4 of 6
The EH Unit staff did not have current and accurate JDs to carry out their roles and responsibilities.	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ A JD is a written statement of facts describing the scope, responsibilities and organizational relationships of a job. It is intended to provide a clear picture of the position's role within the organization. ■ The Human Resource Manual recommended JDs be reviewed every 5 years or at times when a new position is established or responsibilities, organizational set up or technology, working conditions have changed to ensure that job duties are still applicable. ■ The Chief EHO and the EHOs JDs were approved on December 2008 and may not reflect changes in the environment, technology and public health inspection standards/practices that occurred since 2008. ■ According to the Chief EHO, the JDs for the EHO job family (Chief EHO and EHO positions) were still current in terms of role and scope, and did not need many changes. The majority of changes were to improve clarity and consistency for the EHO job family, and bring the format in line with current GNWT format. ■ Management indicated that work had been started to draft new JDs for the Chief EHO and EHO in 2014 in consultation with the Department of Human Resources Job Evaluation Unit. The JDs were still in the process of being finalized. ■ The Executive Assistant's JD was last updated in 2001 and did not reflect her current duties and responsibilities. Management explained the Executive Assistant's JD was scheduled for updating in 2014, however, the updates were deferred until the JDs for the Chief EHO and EHO were finalized. 	
<p>Risk:</p> <ul style="list-style-type: none"> ■ Outdated JDs may result in improper employee compensation, labour grievances, and employees may not be accountable for their actions or performance. 	
<p>Management Action Plan:</p> <ul style="list-style-type: none"> a) By June 2016, management will update JDs to ensure job duties are current and accurate, and establish a process to review JDs that meets requirements as set out in the GNWT Human Resource Manual. 	

Observation 5: Collection and Analysis of Program Information	5 of 6
<p>The Department did not collect complete accurate, relevant, reliable and timely health inspection program information for management and staff to make informed decisions.</p>	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ According to the GNWT Information Technology (IT) Policy and Procedures, Departments must ensure that electronic information is accurate, reliable, current, authentic, and retain its integrity over time. ■ Management explained the current information database was developed in-house by the Department Information Services (IS) staff in 2009 because the former information database was corrupted during the transfer of the EH Unit from Stanton Territorial Hospital to the Department. The intended purpose of the database was to collect all of the inspection results and remove the need for the manual file system. ■ Management indicated that the database lacked built-in programming to assist with data integrity and validation when entering data. This had created issues with the database information which had a negative impact on the ability to effectively manage inspection activities by individual EHOs and the EH unit overall. For example, not clearly defining database columns and not having auto-checking or auto-populating functionality had resulted in a number of data integrity issues such as using different names for the same facility (e.g., "Ecole JH Sissons" and "JH Sissons"); and differentiating permit numbers by adding a negative (-) sign for non-food establishment permit numbers. ■ Data analysis showed 20% of approximately 2,300 transactions in the database had no previous inspection date for food establishments. Management and the Chief EHO have indicated this may be a result of IS / database programming challenges for data extraction and report generation. ■ The Executive Assistant (Assistant) had a key role within the EH Unit to enter inspection results into the database and generate print reports. There was no indication that the data entries were verified for completeness. During staff absences, there was minimal to no coverage for database updates and reports were not processed. Cross training of EHOs and other administrative staff in the Population Health Division was requested by management in 2014; however, this training has not been completed. ■ The Assistant indicated EHOs would sometimes forget to submit the inspection results for entry into the database. Normally these inspection results should be submitted within 5 days. In addition to reminders (as and when basis), the quarterly review of inspection activities was a means to verify missing or overdue inspection reports. ■ Except for rabies complaints, the EH unit stopped tracking all the other complaints in the database after August 2013. 	
<p>Risk:</p> <ul style="list-style-type: none"> ■ Chief EHO unable to assess compliance with the relevant legislation, or monitor and manage the EH Unit effectively. 	
<p>Management Action Plan:</p> <ol style="list-style-type: none"> a) By April 2016, management, in consultation with the Department IS staff, identify and implement improvements to the existing inspection database to mitigate data entry errors and improve accuracy and usefulness of reports. b) By April 2017, management, in consultation with a SME and the Department IS staff, conduct an information needs assessment of IT/IS needs for the EH Unit including a review of other jurisdictions. c) Pending needs assessment outcomes and availability of IT/IS funding and resources, implement a contemporary, cost effective and sustainable information system for environmental health inspection program that reflects both NWT business requirements and best practice in the environmental health field. 	

Observation 6: Retention and Availability of Program Information	6 of 6
<p>The Department management did not have good information to inform, direct, manage and monitor the activities of the EH Unit.</p>	
<p>Issue/Condition:</p> <ul style="list-style-type: none"> ■ Recorded information management helps program managers deliver programs and services to the public and to government and supports the operations of the department. Recorded information supports decision-making and maintains government accountability to the public for its actions. ■ In May 2015, the Minister of the Department was provided information on the current status of inspections, "NWT Environmental Health Inspection Program QUESTIONS & ANSWERS". The information stated that the EH Unit inspected more than 1,300 facilities. In July 2015, data analysis identified 929 facilities. The difference in inspection numbers is a reflection of the database challenges associated with data entry, integrity and analysis functions described in Observation 5. ■ A report from the database that would provide a complete picture of the inspection status was not available due to the database challenges described. Therefore, the number of overdue inspections at any point in time was not readily available to the Chief EHO. ■ According to the Chief EHO, all EHOs have read only access to database. One EHO in a regional office did not use the database and was provided status information from the main office for quarterly reviews or upon request. ■ The EH Unit also had a manual (paper-based) filing system but the Chief EHO explained it was not complete. According to the Chief EHO, in the absence of a fully functional information system to manage inspection activities and documents, the EH Unit should establish a file for each food establishment premise. The file would contain all relevant documents relating to the food establishment premise including the permit application, inspection reports, correspondence, copies of permits and closure documents. ■ The decentralized EH offices in the regions presented a challenge in managing the hardcopy records. For example, some of the food establishment premise documents were in the regional offices and not at headquarters. ■ An approved records retention schedule existed for the EH program area; however, it was dated. Records management improvements have been underway since 2013, including a review of the retention schedule in 2014 that was nearing completion. 	
<p>Risk:</p> <ul style="list-style-type: none"> ■ Record classification and retention may not meet the GNWT ORCS and ARCS requirements ■ The Chief EHO unable to assess compliance with the relevant legislation and regulations, and monitor and manage the EH Unit effectively 	
<p>Management Action Plan:</p> <ol style="list-style-type: none"> a) By December 2016, management and Chief EHO to complete the review of the EH Unit's current records classification system to meet the GNWT ORCS and ARCS requirements. b) By March 2016, Chief EHO to complete the review and consolidation of records for active premises requiring inspections. c) After the information system (Observation 5) improvements have been implemented, management and Chief EHO to use the information to manage and monitor the activities of the EH Unit. 	

E. ACKNOWLEDGEMENT

We would like to thank the staff in the Department for their assistance and co-operation during the audit.



T. Bob Shahi
Director

**Environmental Health Inspection Program
January 2009 to August 2015**

Environmental Public Health Areas of Inspection

Public Health Act and Regulations*

1. Food safety
2. Drinking water safety
3. Communicable disease investigation (enteric diseases; rabies/animal contact investigation)
4. Recreational water
5. Solid waste disposal
6. Public sewerage systems and liquid waste disposal
7. Personal services inspection program (tattooist, piercers, barbers, nail salons, etc)
8. Facilities inspections (public pools, arenas, etc)
9. Tourist establishments
10. Work camps (mining and development exploration camps)
11. Residential rental housing
12. Public school facilities.

Tobacco Control Act and Regulations*

13. Retail tobacco premises

Child Day Care Act and Regulations*

14. Licenced child day care

*EHOs also conduct complaint-based investigations under all of these areas in addition to routine inspections.



MAR 07 2017

CONFIDENTIAL

File: 7820-21-HSS-151-137

MS. DEBBIE DELANCEY
DEPUTY MINISTER
HEALTH & SOCIAL SERVICES

Health and Social Services Authorities Overtime Audit Report

Enclosed is the above referenced Audit Report.

The Internal Audit Bureau will schedule a future follow-up audit. However, in the interim, we would like to be notified of any progress in implementing the changes to regulations, policy, or practices by October 31, 2017.

Should you have any questions concerning the Audit Report, please contact me at (867) 767-9175, Ext. 15215.

T. Bob Shahi
Director

Enclosure

- c. Mr. Jamie Koe, Chair, Audit Committee
Ms. Jeannie Mathison, Director, Finance, HSS



Health and Social Services

Health and Social Services Authorities Overtime
April 1, 2009 to March 31, 2015

Internal Audit Bureau – Audit Report
March 2017



Audit Report Operational Audit

Health and Social Services Health and Social Services Authorities Overtime April 1, 2009 to March 31, 2015

March 2017

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.



March 7, 2017

CONFIDENTIAL

File: 7820-21-HSS-151-137

MS. DEBBIE DELANCEY
DEPUTY MINISTER
HEALTH AND SOCIAL SERVICES

Audit Report: Health and Social Services Authorities, Overtime Audit
Audit Period: April 1, 2009 to March 31, 2015

A. SCOPE AND OBJECTIVES

The Audit Committee Chair approved the Department of Health and Social Services (Department) management request for an audit of the Health and Social Services Authorities' (Authorities) overtime expenditures. The audit focused on the administration of overtime in the Authorities by examining the internal controls for the governance framework, information integrity, compliance and asset safety. The objectives of the audit were to determine if:

- overtime policies and protocols were established and communicated to Authority staff and management.
- information used to make decisions was relevant, reliable, accurate, complete and timely.
- overtime practices were in compliance with Union of Northern Workers (UNW) Collective Agreement, Human Resource Manual (HRM), and the Excluded Employees' Handbook.
- occupational health and safety were given adequate consideration in the approval of overtime.
- the use of overtime compensation facilitated the efficiency and effectiveness of the GNWT and its mandate.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

B. BACKGROUND

The Department promoted, protected and provided for the health and well-being of the people of the Northwest Territories through eight Authorities. Each Authority operated as an independent entity that reported directly to the Minister of Health and Social Services. The Department provided over \$250 million annually to the Authorities through various contribution agreements.

Salaries and benefits were a significant and major cost for Authorities in executing their mandate. The funding of the eight Authorities from the Department included limited funding for overtime.

The Department of Human Resources (DHR) was responsible for the dissemination of the GNWT overtime governance framework, which was accomplished primarily through the HRM. The overtime governance framework prescribed within the HRM applied to all Authorities except for Hay River who operated under a separate Collective Agreement.

The earning and approving of overtime was tracked within PeopleSoft, the primary Enterprise Resource Planning (ERP) system used across Authorities, with the exception of Hay River who used an ERP system known as Ormed (rebranded as VIRTUO MIS). The audit classified overtime as all wages earned above an employee's regular hourly wage. Overall, there were 81 PeopleSoft codes classified as overtime, which included items such as Call Back, Lieu Time, sick relief, electronic call back, and Standby premiums.

HRM requires that the earning of overtime must be authorized in advance by the responsible manager/approving officer. After the overtime has been worked, the employee shall data enter the overtime and note the reasons in the Comments field. Before approving overtime, approving officers must review and confirm the reasons for the overtime provided by the employee in the Comments field. Upon confirming the reason for the overtime, and that the overtime was compliant with the GNWT policy framework, it was approved within PeopleSoft.

C. OVERVIEW

The challenge of delivering 24/7 health and social services throughout the NWT was a high risk endeavor for both the Department and the Authorities. The matching internal control capacity to manage this risk was not evident when we reviewed the overtime practices in all eight Authorities.

There was adequate direction given to staff on recording and approving overtime through the governance framework disseminated by DHR. Improvement of how overtime policy changes were disseminated by DHR to GNWT departments was warranted. However, a governance framework specific to scheduling workers on a 24/7 schedule did not exist. Staff in each Authority used their own initiative to schedule work without a clear mandate.

The overtime expenditure has been increasing over the last six years due to a number of reasons. In 2014-2015, approximately \$15 million in overtime was paid, an increase of 30% from 2009-2010 (**Schedule I refers**). Over 50% of the overtime was in three areas: Overtime, Standby, and Lieu Time (**Schedule I refers**). The underlying cause for this overtime was not susceptible to audit analysis. PeopleSoft provides for employees to record the required information in the "Comment" field and supervisors to review this information before approving overtime. Data analysis shows that the recorded information in PeopleSoft was incomplete or not relevant in over 64% of cases. Some Authorities had, however, established manual systems as an alternative to track justification for overtime.

Data analysis of Lieu Time showed that over 4,000 hours were annually banked by employees beyond the 75 hour maximum allowed under the HRM. This was further compounded by accumulating Call Back/Standby time at a rate of 7,000 hours annually. The impact of both actions was a need for additional staff hours to cover those positions when they drew down on the Lieu Time and Call Back/Standby time.

Enhancement of 24/7 scheduling governance framework, collection of overtime information that was susceptible to rigorous analysis and compliance to existing HRM governance framework will allow the Department and Authorities to make an assessment of effectiveness and efficiency of paid overtime.

D. OBSERVATIONS AND RECOMMENDATIONS

1. Scheduling Framework

Authorities did not have the tools to effectively allocate millions of salary dollars for 24/7 operations due to ad hoc and informal scheduling practices.

There were no international or Canadian standards for the formulation of 24/7 shifts within the health care industry. Operational tempo, resource availability, and labour practices vary widely in the delivery of 24/7 health and social services, and demand that schedules be highly tailored for local considerations. Notwithstanding, a common body of research underscores that many common objectives must be considered when formulating schedules in a 24/7 operational environment, including minimizing total human resource expense (including overtime), maximizing employee preferences and requests, effectively distributing workload, and respecting workplace agreements in policies or negotiated contracts.

The audit observed that 24/7 schedules were formulated without any documented strategy endorsed by the Authorities' executive management. Proposed schedules prepared by front line supervisors were subject to employee challenge when actual or perceived scheduling conflict occurred.

We noted that scheduling methodologies were biased toward maximizing employee preferences while subordinating other objectives, such as minimizing human resource expenses. For example, one section at Stanton established their schedule with the primary goal of maximizing employees' preferences of ensuring a periodic seven-day off break would occur.

Data analysis identified 14 employees in 2014-2015 whose overtime earnings exceed 40% of their base pay (**Schedule II refers**). The overtime paid ranged from \$36,000 to \$145,000 (40% to 190%) on top of regular salary. While scheduling may have been a factor in this overtime, other factors contributing to the overtime included:

- the only employee providing services in the community.
- the need to provide services outside of normal work hours to meet client needs and expectations.
- knowledge, skills and abilities required to perform some responsibilities reside in one person.

The financial impact of overtime was quantifiable at about \$15 million annually. The impact of overtime on Authorities operations (i.e. occurrence

of error, operational efficiency, etc.) and the impact on individual employee’s occupational health and safety were unknown.

Risk Profile

Risk Impact	Major impact requiring detailed research of 24/7 scheduling and management planning by senior management.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	<ul style="list-style-type: none"> • Assistant Deputy Minister, Corporate Services • Assistant Deputy Minister, Territorial Health Programs • Assistant Deputy Minister, Families and Communities • Chief Executive Officer – NTHSSA, TCSA, HRHSSA • Director of Operations (or equivalent) – NTHSSA, TCSA, HRHSSA • Individuals designated to formulate specific Authority schedules.

Recommendation

We recommend that the Department work with the Authorities’ executive management in:

- a) developing a formal framework for 24/7 scheduling that meets the overall goals and objectives of the Department and Authorities.
- b) monitoring the effectiveness of the scheduling framework for its impact on Authorities’ operations and employees occupational health.

Management Response

Action Plan	Completion Date
The Department agrees with the recommendation to develop a formal framework for 24/7 scheduling that meets the overall goals and objectives of providing safe care, efficiently and effectively. The Department will work with NTHSSA, TSCA and HRHSSA on an action plan to develop a formal scheduling framework.	April 2019

2. PeopleSoft Overtime Approval

Over 64% of overtime approved in PeopleSoft had inadequate information to determine the need for overtime.

HRM 0604, para 8, requires that the employee shall note the reasons for the overtime in the Comments field within PeopleSoft. In turn, HRM 0604, para 7, requires that the approving officer must review and confirm the reasons for the overtime provided by the employee in the Comments field of PeopleSoft. PeopleSoft was the approved ERP application for recording, tracking and monitoring of overtime.

Across the four Authorities' where fieldwork was conducted, we witnessed a multitude of systems in use to justify and approve overtime, such as chits, email, text, verbal, and sign-in logs. While the audit confirmed some sections diligently use a chit/voucher system to track the specific reason and approval authority for overtime, it was the general opinion of interviewed staff that over 50% of all authorization to work overtime was verbal. Verbal authorization was compliant with HRM policy, however did not provide a clear audit trail that could be reviewed that documented the reason for the overtime or who preapproved the requirement for overtime.

PeopleSoft data analysis revealed that the Comments field within PeopleSoft was not completed in 64% of the time when overtime was recorded as earned and approved (128,500 of 199,600 entries). A central repository of overtime justification was not tracked in PeopleSoft. The specific requirements delineated in HRM 604 were not well known and there was no mechanism for senior managers to assess compliance. Management had allowed alternative systems to approve overtime without the appropriate capacity to analyze the information. Justification of overtime funding required to sustain Authorities' operations was not based on objective, verifiable evidence.

Risk Profile

Risk Impact	Moderate impact requiring specific allocation of responsibility for the risk.
Risk Responsibility	<ul style="list-style-type: none"> • Chief Executive Officer – NTHSSA, TCSA, HRHSSA
Risk Mitigation Support	<ul style="list-style-type: none"> • Director of Operations – NTHSSA, TCSA, HRHSSA • All earners and approvers of overtime within the Authorities

Recommendation:

We recommend that the Department have the Authorities' provide the reasons for overtime that can be analyzed and verified by the Department to support the request for additional funding stemming from overtime.

Management Response:

Action Plan	Completion Date
The Department in consultation with NTHSSA, HRHSSA and TCSA will review and implement an appropriate process to ensure reasons for overtime are recorded and that useful data is then available for analysis. HSS will consult with GNWT partners (Department of Human Resources, Department of Finance Informatics Shared Services) during review for options and to promote consistency across GNWT.	October 2018

3. Banked Time

Over 35,000 hours of overtime, call-back, and standby was banked for future paid leave from work.

Current GNWT policy allows compensation for overtime to be taken as cash payment or lieu time. HRM 609, lieu time, para 5, specifies that, "Employees may not accumulate more than 75 hours of lieu time per fiscal year (80 hours for employees who work eight hour days)". If the employee has reached their maximum lieu time for the fiscal year (75/80 hours), HRM 609, para 7, stipulates that the employee will automatically be compensated for the overtime as a cash payment on his/her pay cheque. With regard to call-back and standby hours, HRM 604a, para 19, specifies that employees, "Obtain authorization for standby or call-back to be compensated as lieu time".

All Authorities were non-compliant with HRM policy 609. Data analysis for the three year period 2013-2015 revealed that Authorities' staff banked overtime, call-back, and standby time as follows:

Year	Lieu time > 75 hours banked (LTE)	Call-back/standby banked (CBE)	Total
2012-2013	4,788	7,820	12,608
2013-2014	3,367	7,265	10,632
2014-2015	4,570	7,968	12,538
Total	12,725	23,053	35,778

The subsequent use of banked time as paid leave from work increased the risk for overtime for those staff remaining in the workplace. For example, in 2014-2015, employees within the Stanton Operating Room section took a combined 3,340 hours of banked leave, with one employee taking 23(2)(d) 23(2)(d). Fewer employees available within a busy and demanding workplace may necessitate increased overtime for the remaining employees to sustain operational demands.

Individuals responsible for approving overtime in PeopleSoft did not ensure the banking of lieu time and call-back/standby time was in compliance with the GNWT governance framework. Notwithstanding the controls and information available within PeopleSoft to all time approvers, such as lieu time hours banked and taken, there were no usage or summary reports requested from DHR to facilitate oversight and compliance with leave bank governance.

Risk Profile:

Risk Impact	Moderate impact requiring allocation of management responsibility to monitor compliance to the HRM.
Risk Responsibility	Director of Finance – NTHSSA, TCSA, HRHSSA
Risk Mitigation Support	<ul style="list-style-type: none"> • Director of Operations – NTHSSA, TCSA, HRHSSA • Department of Finance – Director Informatics Shared Services • PeopleSoft time approvers • DHR Client Manager.

Recommendation

We recommend that the Department work with Authorities to establish a process to allow the Authority DFAs to:

- a. in conjunction with Directors’ of Operations, remind PeopleSoft time approvers about the requirement of HRM 609.
- b. liaise with DHR to establish a GNWT governance framework for PeopleSoft time code Call Back Earned (CBE).
- c. review all leave bank reports on a regular basis for compliance and brief CEO/Director of Operations on status of any non-compliance.

Management Response

Action Plan	Completion Date
<p>The Department agrees with the recommendation and in consultation with NTHSSA, HRHSSA and TCSA will review and take steps to ensure that the HRM 0609 is followed in the Authorities.</p> <p>The Department agrees that a GNWT governance framework for Call Back Earned is required and will support the DHR, upon completion of the GNWT Overtime Audit currently underway, as it leads the establishment of the required framework. DHSS will ensure compliance with the framework once implemented.</p>	April 2019

E. ACKNOWLEDGEMENT

We would like to thank the staff at DHSS and at the Authorities for their assistance and co-operation during the audit.

A handwritten signature in blue ink, appearing to read 'T. Bob Shahi', with a stylized flourish at the end.

T. Bob Shahi
Director

Health and Social Services
Health and Social Services Authorities' Overtime

GNWT Health and Social Services Authorities						
Overtime Earnings by Health Authority 2009-2015						
Health Authority	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015
Stanton	\$ 4,735,591	\$ 4,338,538	\$ 4,845,775	\$ 5,517,153	\$ 6,067,162	\$ 6,531,186
Tlicho	\$ 906,016	\$ 969,493	\$ 937,323	\$ 1,030,665	\$ 1,078,294	\$ 1,211,943
Dehcho	\$ 933,902	\$ 909,744	\$ 944,733	\$ 1,011,817	\$ 1,092,757	\$ 1,036,404
Beaufort-Delta	\$ 1,914,588	\$ 1,841,906	\$ 1,948,413	\$ 1,892,638	\$ 2,423,966	\$ 2,233,135
Yellowknife	\$ 729,944	\$ 781,765	\$ 740,496	\$ 743,399	\$ 828,341	\$ 960,547
Fort Smith	\$ 937,450	\$ 1,330,215	\$ 1,567,340	\$ 1,396,648	\$ 1,449,081	\$ 1,258,835
Sahtu	\$ 727,837	\$ 851,529	\$ 790,240	\$ 888,632	\$ 858,240	\$ 856,970
Hay River	\$ 676,095	\$ 751,096	\$ 658,866	\$ 744,775	\$ 826,348	\$ 825,000
Total	\$ 11,561,423	\$ 11,774,286	\$ 12,433,187	\$ 13,225,728	\$ 14,624,190	\$ 14,914,020

* Note

* Note: Hay River Overtime estimated for Fiscal Year 2014-2015 based on previous year, as data analysis limited to 5 year period 2010-2014 only.

GNWT HSSA							
Top Five Types of Overtime**							
2009-2015							
PeopleSoft Code	Type of Overtime	2009-2010	2010-2011	2011-2012	2012-2013	2013-2014	2014-2015
OT1	Overtime @ 1.5 4/6/8U	\$ 1,616,801	\$ 1,547,532	\$ 1,589,900	\$ 1,600,484	\$ 1,858,257	\$ 1,930,169
OT2	Overtime @ 2.0	\$ 1,575,344	\$ 1,441,306	\$ 1,917,842	\$ 1,812,201	\$ 1,918,071	\$ 1,917,007
SBU	Stndby Unwrkd 4/6/8U 1.5X HR	\$ 1,323,630	\$ 1,399,693	\$ 1,495,771	\$ 1,594,177	\$ 1,663,935	\$ 1,770,278
SBW	Standby Wrkd 4/6/8U 1X HR	\$ 1,106,593	\$ 1,152,203	\$ 1,197,358	\$ 1,234,125	\$ 1,229,210	\$ 1,246,455
LT2	Lieu Hours Taken 8U	\$ 731,798	\$ 726,597	\$ 813,018	\$ 852,337	\$ 900,987	\$ 892,071
	Total	\$ 6,354,165	\$ 6,267,331	\$ 7,013,888	\$ 7,093,325	\$ 7,570,460	\$ 7,755,981
	Percent of Total Overtime Approved (exclusive of Hay River)	58%	57%	60%	57%	55%	55%

**: Exclusive of Hay River, as specific type of overtime within Hay River HSSA was not included in data analysis.

**Health and Social Services
Health and Social Services Authorities' Overtime**

GNWT Health Authorities: Positions with Persistent Earning of Overtime

2013-2015

Position Number	Position Title	HSSA	Overtime Earned in 2014-2015	2015 Pay Level of Current Incumbant	Current Annual Earnings of Incumbant based on 1,950 hrs	Overtime Earnings as % of Regular Pay Level
23(2)(d)		Tlicho	23(2)(f)			
		Stanton				
		Tlicho				
		Stanton				
		Stanton				
		Tlicho				
		Stanton				
		Stanton				
		Stanton				
		Fort Smith				
		Stanton				
		Stanton				



MAY 30 2018

CONFIDENTIAL

File: 7820-20-GNWT-151-131

MR. BRUCE COOPER
DEPUTY MINISTER
HEALTH AND SOCIAL SERVICES

Access to Information and Protection of Privacy Assessment

Enclosed is the above referenced Assessment.

We will schedule a follow-up in the future to determine the progress of the agreed upon Management Action Plan. However, we would appreciate an update by November 2018 on the status of the management action plan.

We would like to thank the staff in the Department for their assistance and co-operation during the audit. Should you have any questions, please contact me at (867) 767-9175, Ext. 15215.

T. Bob Shahi
Director, Internal Audit Bureau
Finance

Enclosure

- c. Mr. Jamie Koe, Chair, Audit Committee
Ms. Jeannie Mathison, Director, Finance, HSS



HEALTH AND SOCIAL SERVICES

Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



HEALTH AND SOCIAL SERVICES

Access to Information and Protection of Privacy Assessment

May 2018

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

**CONFIDENTIAL**

May 30, 2018

File: 7820-20-GNWT-151-131

MR. BRUCE COOPER
DEPUTY MINISTER
HEALTH AND SOCIAL SERVICES

Audit Report: Access to Information and Protection of Privacy Assessment
Audit Period: As of March 31, 2018

A. SCOPE AND OBJECTIVES

The Audit Committee approved the GNWT wide operational audit of Access to Information and Protection of Privacy (ATIPP) legislation that focused on privacy of information.

An assessment of Health & Social Services was part of the GNWT wide audit project. This report identifies issues specific to your department.

In assessing the privacy of information for all the departments, a number of recommendations impacted more than one department. These items were reported in the "*Corporate Privacy Report*" and forwarded to the Department of Justice for further action. A copy of this report forms part of the "*Corporate Privacy Report*".

B. BACKGROUND

The 1996 *ATIPP Act* plays a critical part in maintaining government accountability and protecting the public's personal information. The legislation treats all public bodies (i.e. – departments, boards, commissions, etc.) as

This report may be subject to request under the Access to Information and Protection of Privacy (ATIPP) Act.

treats all public bodies (i.e. – departments, boards, commissions, etc.) as separate entities. The GNWT currently employs a decentralized approach where each public body has a designated access and privacy coordinator. The Department of Justice Access and Privacy Office (APO) provides government-wide support and leadership to public bodies in complying with the *ATIPP Act*.

Crowe MacKay LLP was awarded a contract through the competitive Request for Proposal process that was evaluated by staff from APO and Internal Audit Bureau (IAB).

C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached audit report, *“Department of Health & Social Services, Access to Information and Protection of Privacy Act (ATIPP) Part 2”*, made a number of observations and recommendations specific to your department (**Schedule I**). The management responses to the recommendations have been incorporated in the attached report.

The contractor assessed the compliance to *ATIPP Act* and Regulations as well as nine privacy principles for your department at three levels:

- **Assessed Maturity** based on the evidence provided by your department.
- **Minimum Maturity** required to be compliance to *ATIPP Act* with a target date of 12 to 24 months.
- **Desired Maturity** indicates maturity that would take over 24 months to achieve.

Overall, the privacy risk for your department was assessed to be “very high” requiring internal control capacity at “optimized” level. The current capacity of the department was “repeatable”, meaning that the processes could be repeated as long as there was no change in staff, policy, procedures or processes. The immediate task for the department was to document privacy processes (defined level). Subsequently, the department can focus on identifying and addressing privacy exceptions through monitoring (managed level) and on-going continuous improvement in the privacy process (optimized level) (**Chart I refers**)

Some of the key recommendations made by the contractor were:

- Working with APO to develop and implement privacy policy.
- Completing an inventory of personal information collected.
- Documenting the privacy processes.

The action plan indicated by management should address the outstanding risks. The IAB will follow-up on the status of the management action plan after six months during our scheduled follow-up audits.

D. ACKNOWLEDGEMENT

We would like to thank the department staff for their assistance and co-operation throughout the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

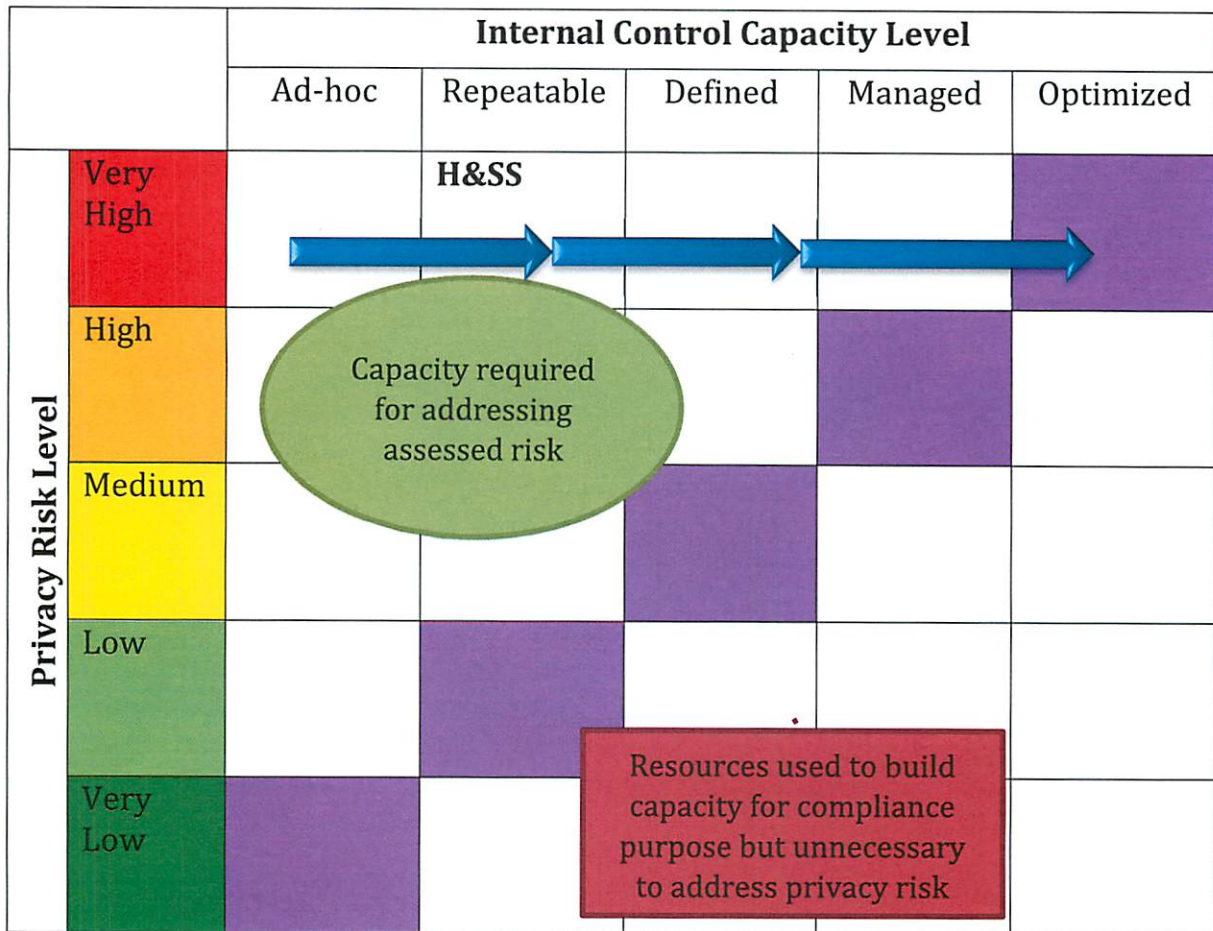
7820-20-GNWT-151-131

Access to Information and Protection of Privacy
As of March 31, 2018

Chart I

Risk and Opportunity Assessment using Capacity Model

An effective Risk Management Program balances the capacity level of internal control (people, process, and technology) with organizational risk.



DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Scope and Objectives

The Government of the Northwest Territories (GNWT) issued a request for proposal, for an operational audit reviewing departmental compliance with Part 2 of the ACCESS to Information and Protection of Privacy Act (ATIPP or “the Act”). Crowe MacKay LLP (Crowe MacKay), being the successful proponent. The work was coordinated directly under the supervision of the Director, Internal Audit Bureau.

Testing of departments was based on the Generally Accepted Privacy Principles (GAPP) which incorporates 10 principles, each backed up by an objective and measurable criteria to determine risk and compliance within each department included in our scope. We reviewed key controls related to each of the principles, taking into account their associated criteria. This testing was conducted on current approaches to and compliance activities of each department.

Preliminary survey determined that the maturity of GNWT’s control environment related to Part 2: Protection of Privacy was less mature than that related to Part 1: Access to Information. Considering the less mature control environment likely in place for most departments, the focus of the audit was adjusted to be less compliance-based and more risk-based with a strong focus on the maturity levels denoted in the AICPA/CICA Privacy Maturity Model (Privacy Maturity Model) (**Appendix A refers**). We relied less on substantive testing of controls already in place and addressed the risks related to effectively establish a sound governance framework by the Access and Privacy Office as well as how each department interpreted this framework for departmental application. With regards to the integrity of information held in the custody of each department, the compilation of that personal information and the thought/opinions provided by each department of their control environment for appropriately protecting this personal information, this audit assessed what was being done in order to gain comfort and provide support for the opinions of each department where possible.

Departmental Background

The Department of Health and Social Services (“HSS”) meets its responsibilities through health and social service programs. In October 2015 the personal information collected by HSS for its health programs became subject to the newly introduced Health Information Act (HIA) which specifies privacy requirements that supersede ATIPP. The department modified its privacy policies established prior to HIA to conform to HIA requirements upon its introduction and the result was that those policies form the HIA privacy policies and procedures. Personal information collected for social services programs is governed by other Acts and regulations that include notwithstanding clauses that result in these Acts superseding ATIPP. The Acts with notwithstanding clauses are the Adoption Act and Child and Family Services Act.

Department information falling under the HIA has been excluded from the scope of this audit.

Due to the fact that the Adoption Act and Child and Family Services Act have not withstanding clauses and the department works to meet each of these legislations, rather than specifically ATIPP, the personal information managed under these acts has also been excluded. The remaining information mostly relates to personnel records and administrative data.

All divisions store information collected in hard copy under the Operational Records Classification System and the Administrative Records Classification System, including electronic information in the Digital Integrated Information Management System (DIIMS).

Overview

Risk Profile

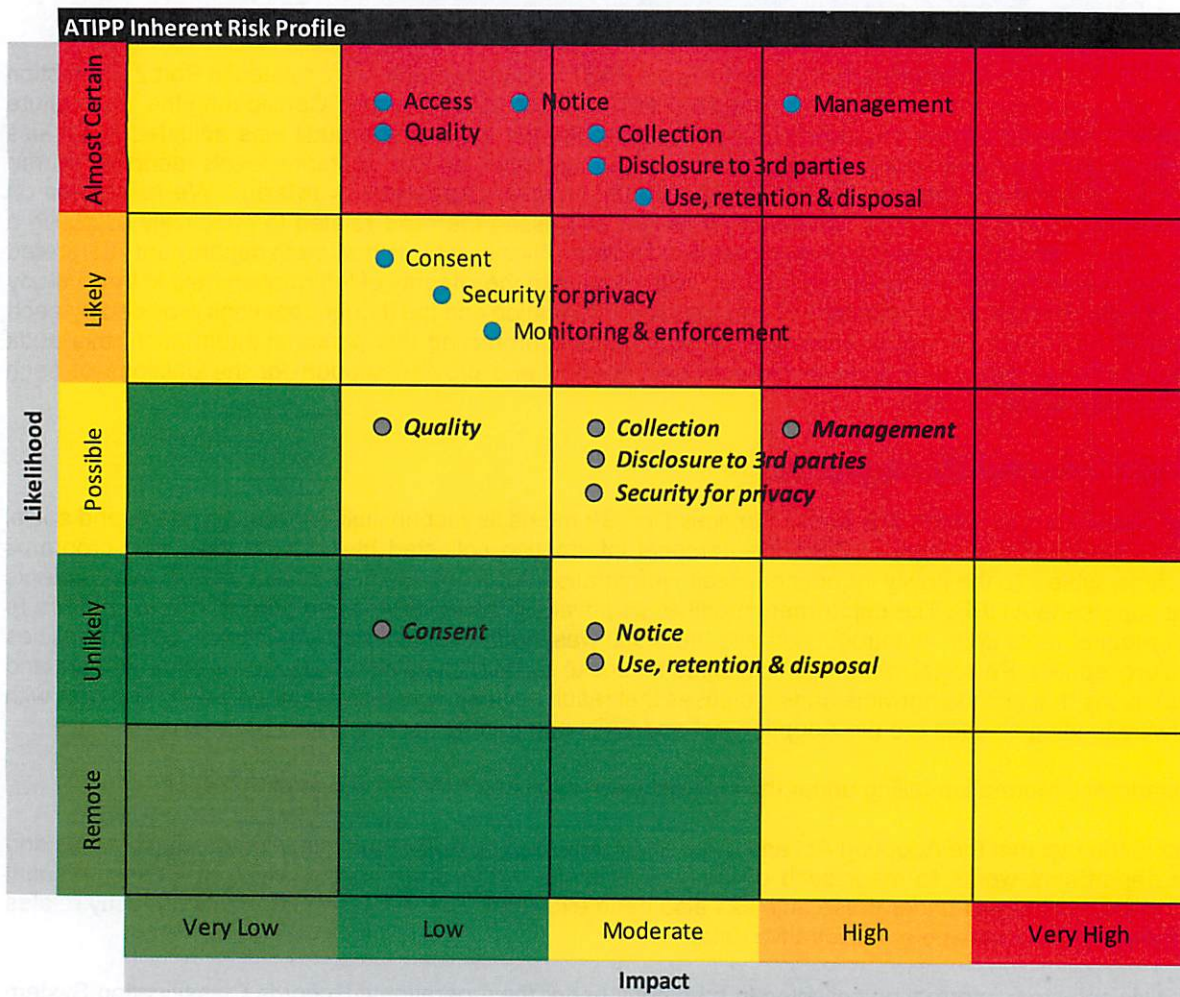
The inherent risk profile per the planning memo, detailed in the heatmap below, was provided to the department ATIPP Coordinator and privacy contacts at the department interview. The planning risk profile

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the IACPA/CICA Privacy Maturity Model. The heatmap shows the initial inherent risk rating for each principle in regular black print as well as our applied rating based on the results of our department review in bold italics. Changes represent recognition of controls implemented by the department which serve to reduce risk. For example, a rating of ad hoc in relation to a principle area would result in no change in the risk map as no controls have yet been implemented. A rating higher in the maturity model will result in an adjustment to the heat map placement and an entry in the new locations denoted by bold and italics.

RISK HEATMAP



Compliance with ATIPP Part 2 Protection of Privacy

An assessment of whether or not the department is compliant with specific requirements of ATIPP legislation has been made. Please refer to Appendix A for a summary of the requirements for each section. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Based on the audit work performed the department is not fully compliant with ATIPP Part 2. Support for this is as follows:

Section	Compliance Assessment	Reason for Non-Compliance
Part 2: Division A – Collection of Personal Information		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	
42	COMPLIANT	
Part 2: Division B – Use of Personal Information		
43	COMPLIANT	
44	COMPLIANT	
45	N/A	An error or omission has not been identified.
46	N/A	An error or omission has not been identified.
Part 2: Division C – Disclosure of Personal Information		
47	COMPLIANT	
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	UNVERIFIED	Full compliance cannot be verified.
49	N/A	No disclosure for research or statistics.
Regulations relating to disclosure of personal information		
5	COMPLIANT	
6	N/A	No formal examination noted.
8	N/A	No research agreement in place.

Maturity Rating against Privacy Maturity Model

Using the Privacy Maturity Model (**Appendix A refers**), the assessed maturity, minimum maturity and desired maturity are illustrated in the graph below.

Assessed Maturity Level – current level of maturity for the department based on the audit.

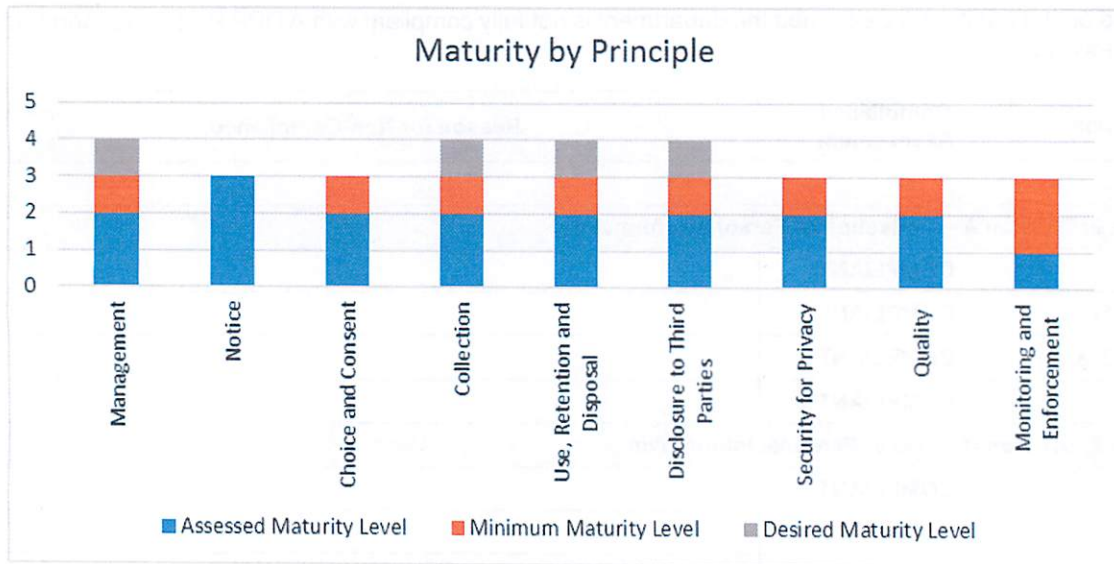
Minimum Maturity Level – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

Desired Maturity Level – This level would be achieved via long term goals (>24 months) and should be part of long term planning if applicable to your department.

Departments with data which is of a sensitive nature or for which there are large amounts of information are expected to reach the minimum maturity level in the short term (12-24 months), as guided by the observations in the report, and then plan to reach the desired maturity level over time in order to ensure adequate protection of data. HSS falls into this category, and is therefore expected to plan for the desired maturity level in the future.

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)



Overall findings, including rating of the department against each privacy principle, is summarized in the following table:

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p>Management</p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Repeatable	<ul style="list-style-type: none"> Privacy policies have not been formally designed and documented to address information not legislated by the Health Information Act (HIA). An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved. An ATIPP Coordinator has been assigned and works within the department's privacy division. ATIPP Coordinator has taken training sessions offered by the GNWT Access and Privacy Office and has past experience as well as knowledge and support within the division. Privacy division within department allows for communication of privacy within department and the development of processes to include privacy unit involvement in new programs. <p><i>See observations 1-2.</i></p>
<p>Notice</p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.</p>	Defined	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address notice to individuals. Notice is provided on all forms used to collect personal information. <p><i>See observation 1.</i></p>

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p>Consent</p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.</p>	<p>Defined</p>	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address consent of individuals. • Implicit consent is obtained on personal information collection forms. • Explicit consent is obtained on information collection forms when sensitive information is collected. <p><i>See observation 1.</i></p>
<p>Collection</p> <p>The department collects personal information only for the purposes identified in the notice.</p>	<p>Repeatable</p>	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address collection of personal information. • The type of personal information collected and the method of collection for personal information collected by forms is known to the individual and the department discloses the collection of information through the use of cookies. • The privacy unit is involved in the review process for all new programs or changes to existing programs that involve the use and collection of personal information (whether ATIPP, HIA, etc.). <p><i>See observations 1.</i></p>
<p>Use, retention and disposal</p> <p>The department limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.</p>	<p>Defined</p>	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address use, retention and disposal. • A procedure/process exists to ensure information collected is only used for the purpose it was collected for. • Retention and disposal of information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the Digital Integrated Information Management System (DIIMs) which allows for information to be retained for no longer than necessary and is disposed of at that time. <p><i>See observation 1.</i></p>
<p>Disclosure to third parties</p> <p>The department discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</p>	<p>Repeatable</p>	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be taken if the information was misused by the third party. • Information sharing agreements exist with other departments and contracts exist with third parties, to provide instructions or requirements

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>to the departments regarding the personal information disclosed, to ensure the information is only used for the purpose for which it was collected and to ensure the information will be protected in a manner consistent the department's requirements.</p> <p><i>See observation 1.</i></p>
<p>Security for privacy</p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address security for privacy. • Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Systems division. • Physical access to personal information is restricted. • Security measures exist over the transmission of data and are documented. • Tests of all safeguards in place are not performed on a regular basis. <p><i>See observation 1.</i></p>
<p>Quality</p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address quality to ensure personal information is complete and accurate for the purposes for which it is to be used and it is relevant to the purposes for which it is to be used. <p><i>See observation 1.</i></p>
<p>Monitoring and enforcement</p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.</p>	Ad Hoc	<ul style="list-style-type: none"> • A privacy policy has not been formally designed and documented to address monitoring and enforcement. • Monitoring and enforcement are not being done at present. <p><i>See observation 3.</i></p>

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Observations and Recommendations

Observation 1

Privacy policy has not been designed and documented

- When HIA was introduced HSS modified and transferred its privacy policies and procedures to form the HIA policy manual which left a lack of policy and procedures to address ATIPP Part 2 for information that does not fall under the HIA.

Risk Profile:

Risk Impact	Without a documented privacy policy, consistent direction cannot be given to departmental personnel which results in inconsistent or non-compliance with ATIPP legislation.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- The Department of Justice develop a GNWT-wide privacy policy and associated guidelines.
- The department should work with Justice to ensure that departmental processes and procedures are set up to allow the department to meet the overarching policy and guidelines.
- This one policy should address requirements as set out within the ATIPP Act, and ensure the privacy principles are sufficiently addressed to meet minimum maturity requirements.

Management Response:

Action Plan	Completion Date:
DHSS agrees with recommendation and will commit employee resources to assist Justice in completing this task.	N/A

Observation 2

An inventory of personal information collected does not exist

- Department staff have knowledge of the personal information collected by their division but it is not documented and a global listing cannot be readily created or obtained.
- Systems involved in collection and storage of personnel information are not documented
- Third parties involved are not documented.

Risk Profile:

Risk Impact	Without an inventory of personal information, it is not possible for the department to ensure that all areas of personal information are correctly protected under ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Recommendations:

We recommend that:

- An inventory of the types of personal information and the related processes, systems, and third parties involved be created by each division and be submitted to the ATIPP Coordinator for consolidation into a global department inventory. A review of all areas should then take place to ensure compliance processes and procedures are in place.

Management Response:

Action Plan	Completion Date:
DHSS agrees with recommendation. The DHSS Health Privacy Unit will lead a departmental wide survey on the collection/use/storage of person information with the assistance of divisional directors. This inventory will include not only personal information protected by the privacy provisions of ATIPP but all personal information and its corresponding legislation i.e. Health Information Act, Child and Family Services Act etc.	December 2018

Observation 3

Monitoring, enforcement and updates are not being performed

- Since the introduction of HIA, ATIPP compliance for areas not under HIA are not being addressed on a regular basis
- Procedures and processes are in place based on policies developed to address ATIPP prior to the existence of HIA that subsequently became HIA policies but reviews and monitoring of those procedures/processes and collection forms for adequacy and compliance with changes in programs and/or legislation is not being done.

Risk Profile:

Risk Impact	Without a review of processes and procedures on an ongoing basis there is a risk of non-compliance with ATIPP legislation.
Risk Responsibility	Assistant Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

Recommendations:

We recommend that:

- A procedure be formalized that requires review of compliance with the department's privacy policies and procedures, laws, regulations, and other requirements.
- A procedure be formalized that addresses how a selection of controls will be monitored and the frequency with which they will be monitored, ideally based on a risk assessment.

Management Response:

Action Plan	Completion Date:
DHSS agrees with recommendation and will complete this task after the Department of Justice has developed the GNWT ATIPP Privacy policies.	TBD based on timing of completion of Department of Justice Privacy policies.

DEPARTMENT OF HEALTH AND SOCIAL SERVICES

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Doing so will ensure the DHSS' procedure will be in line with the new GNWT ATIPP policies.	
--	--

Responses provided by Michele Herriot with a copy to Jennifer Howie. Responses were reviewed by the DM.

AICPA/CICA Privacy Maturity Model

March 2011



Notice to Reader

DISCLAIMER: This document has not been approved, disapproved, or otherwise acted upon by any senior technical committees of, and does not represent an official position of the American Institute of Certified Public Accountants (AICPA) or the Canadian Institute of Chartered Accountants (CICA). It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this document. The services of a competent professional should be sought when legal advice or other expert assistance is required.

Neither the authors, the publishers nor any person involved in the preparation of this document accept any contractual, tortious or other form of liability for its contents or for any consequences arising from its use. This document is provided for suggested best practices and is not a substitute for legal advice. Obtain legal advice in each particular situation to ensure compliance with applicable laws and regulations and to ensure that procedures and policies are current as legislation and regulations may be amended.

Copyright©2011 by
American Institute of Certified Public Accountants, Inc.
and Canadian Institute of Chartered Accountants.

All rights reserved. Checklists and sample documents contained herein may be reproduced and distributed as part of professional services or within the context of professional practice, provided that reproduced materials are not in any way directly offered for sale or profit. For information about the procedure for requesting permission to make copies of any part of this work, please visit www.copyright.com or call (978) 750-8400.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA

Vice Chair

Kenneth D. Askelson, CPA, CITP, CIA

Eric Federing

Philip M. Juravel, CPA, CITP

Sagi Leizerov, Ph.D., CIPP

Rena Mears, CPA, CITP, CISSP, CISA, CIPP

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

Doron M. Rotman, CPA (Israel), CISA, CIA, CISM, CIPP

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

Staff Contacts:

Nicholas F. Cheung, CA, CIPP/C

CICA

Principal, Guidance and Support

and

Nancy A. Cohen, CPA, CITP, CIPP

AICPA

Senior Technical Manager, Specialized Communities and Practice Management

Acknowledgements

The AICPA and CICA appreciate the contributions of the volunteers who devoted significant time and effort to this project. The institutes also acknowledge the support that the following organization has provided to the development of the Privacy Maturity Model:



Table of Contents

- 1 Introduction 1**
- 2 AICPA/CICA Privacy Resources 1**
 - Generally Accepted Privacy Principles (GAPP)..... 1
 - Privacy Maturity Model..... 2
- 3 Advantages of Using the Privacy Maturity Model 2**
- 4 Using the Privacy Maturity Model 2**
 - Getting Started..... 3
 - Document Findings against GAPP..... 3
 - Assessing Maturity Using the PMM 3
- 5 Privacy Maturity Model Reporting 3**
- 6 Summary..... 4**
- AICPA/CICA PRIVACY MATURITY MODEL**
- Based on Generally Accepted Privacy Principles (GAPP) 5**

Appendix A

AICPA/CICA Privacy Maturity Model

This page intentionally left blank.

AICPA/CICA Privacy Maturity Model User Guide

1 INTRODUCTION

Privacy related considerations are significant business requirements that must be addressed by organizations that collect, use, retain and disclose personal information about customers, employees and others about whom they have such information. **Personal information** is information that is about, or can be related to, an identifiable individual, such as name, date of birth, home address, home telephone number or an employee number. Personal information also includes medical information, physical features, behaviour and other traits.

Privacy can be defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

Becoming privacy compliant is a journey. Legislation and regulations continue to evolve resulting in increasing restrictions and expectations being placed on employers, management and boards of directors. Measuring progress along the journey is often difficult and establishing goals, objectives, timelines and measurable criteria can be challenging. However, establishing appropriate and recognized benchmarks, then monitoring progress against them, can ensure the organization's privacy compliance is properly focused.

2 AICPA/CICA PRIVACY RESOURCES

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed tools, processes and guidance based on **Generally Accepted Privacy Principles (GAPP)** to assist organizations in strengthening their privacy policies, procedures and practices. GAPP and other tools and guidance such as the AICPA/CICA Privacy Risk Assessment Tool, are available at www.aicpa.org/privacy and www.cica.ca/privacy.

Generally Accepted Privacy Principles (GAPP)

Generally Accepted Privacy Principles has been developed from a business perspective, referencing some but by no means all significant local, national and international privacy regulations. GAPP converts complex privacy requirements into a single privacy objective supported by 10 privacy principles. Each principle is supported by objective, measurable criteria (73 in all) that form the basis for effective management of privacy risk and compliance. Illustrative policy requirements, communications and controls, including their monitoring, are provided as support for the criteria.

GAPP can be used by any organization as part of its privacy program. GAPP has been developed to help management create an effective privacy program that addresses privacy risks and obligations as well as business opportunities. It can also be a useful tool to boards and others charged with governance and the provision of oversight. It includes a definition of privacy and an explanation of why privacy is a business issue and not solely a compliance issue. Also illustrated are how these principles can be applied to outsourcing arrangements and the types of privacy initiatives that can be undertaken for the benefit of organizations, their customers and related persons.

The ten principles that comprise GAPP:

- **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
- **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
- **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
- **Collection.** The entity collects personal information only for the purposes identified in the notice.
- **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
- **Access.** The entity provides individuals with access to their personal information for review and update.
- **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

- **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
- **Quality.** The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
- **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Since GAPP forms the basis for the Privacy Maturity Model (PMM), an understanding of GAPP is required. In addition, an understanding of the entity's privacy program and any specific privacy initiatives is also required. The reviewer should also be familiar with the privacy environment in which the entity operates, including legislative, regulatory, industry and other jurisdictional privacy requirements.

Privacy Maturity Model

Maturity models are a recognized means by which organizations can measure their progress against established benchmarks. As such, they recognize that:

- becoming compliant is a journey and progress along the way strengthens the organization, whether or not the organization has achieved all of the requirements;
- in certain cases, such as security-focused maturity models, not every organization, or every security application, needs to be at the maximum for the organization to achieve an acceptable level of security; and
- creation of values or benefits may be possible if they achieve a higher maturity level.

The AICPA/CICA Privacy Maturity Model¹ is based on GAPP and the Capability Maturity Model (CMM) which has been in use for almost 20 years.

The PMM uses five maturity levels as follows:

1. Ad hoc – procedures or processes are generally informal, incomplete, and inconsistently applied.
2. Repeatable – procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.

¹ This model is based on Technical Report, CMU/SEI-93TR-024 ESC-TR-93-177, "Capability Maturity Model SM for Software, Version 1.1," Copyright 1993 Carnegie Mellon University, with special permission from the Software Engineering Institute. Any material of Carnegie Mellon University and/or its Software Engineering Institute contained herein is furnished on an "as-is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement. This model has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute. Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

3. Defined – procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. Managed – reviews are conducted to assess the effectiveness of the controls in place.
5. Optimized – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

In developing the PMM, it was recognized that each organization's personal information privacy practices may be at various levels, whether due to legislative requirements, corporate policies or the status of the organization's privacy initiatives. It was also recognized that, based on an organization's approach to risk, not all privacy initiatives would need to reach the highest level on the maturity model.

Each of the 73 GAPP criteria is broken down according to the five maturity levels. This allows entities to obtain a picture of their privacy program or initiatives both in terms of their status and, through successive reviews, their progress.

3 ADVANTAGES OF USING THE PRIVACY MATURITY MODEL

The PMM provides entities with a useful and effective means of assessing their privacy program against a recognized maturity model and has the added advantage of identifying the next steps required to move the privacy program ahead. The PMM can also measure progress against both internal and external benchmarks. Further, it can be used to measure the progress of both specific projects and the entity's overall privacy initiative.

4 USING THE PRIVACY MATURITY MODEL

The PMM can be used to provide:

- the status of privacy initiatives
- a comparison of the organization's privacy program among business or geographical units, or the enterprise as a whole
- a time series analysis for management
- a basis for benchmarking to other comparable entities.

To be effective, users of the PMM must consider the following:

- maturity of the entity's privacy program
- ability to obtain complete and accurate information on the entity's privacy initiatives
- agreement on the Privacy Maturity assessment criteria
- level of understanding of GAPP and the PMM.

Getting Started

While the PMM can be used to set benchmarks for organizations establishing a privacy program, it is designed to be used by organizations that have an existing privacy function and some components of a privacy program. The PMM provides structured means to assist in identifying and documenting current privacy initiatives, determining status and assessing it against the PMM criteria.

Start-up activities could include:

- identifying a project sponsor (Chief Privacy Officer or equivalent)
- appointing a project lead with sufficient privacy knowledge and authority to manage the project and assess the findings
- forming an oversight committee that includes representatives from legal, human resources, risk management, internal audit, information technology and the privacy office
- considering whether the committee requires outside privacy expertise
- assembling a team to obtain and document information and perform the initial assessment of the maturity level
- managing the project by providing status reports and the opportunity to meet and assess overall progress
- providing a means to ensure that identifiable risk and compliance issues are appropriately escalated
- ensuring the project sponsor and senior management are aware of all findings
- identifying the desired maturity level by principle and/or for the entire organization for benchmarking purposes.

Document Findings against GAPP

The maturity of the organization's privacy program can be assessed when findings are:

- documented and evaluated under each of the 73 GAPP criteria
- reviewed with those responsible for their accuracy and completeness
- reflective of the current status of the entity's privacy initiatives and program. Any plans to implement additional privacy activities and initiatives should be captured on a separate document for use in the final report.

As information on the status of the entity's privacy program is documented for each of the 73 privacy criteria, it should be reviewed with the providers of the information and, once confirmed, reviewed with the project committee.

Assessing Maturity Using the PMM

Once information on the status of the entity's privacy program has been determined, the next task is to assess that information against the PMM.

Users of the PMM should review the descriptions of the activities, documents, policies, procedures and other information expected for each level of maturity and compare them to the status of the organization's privacy initiatives.

In addition, users should review the next-higher classification and determine whether the entity could or should strive to reach it.

It should be recognized that an organization may decide for a number of reasons not to be at maturity level 5. In many cases a lower level of maturity will suffice. Each organization needs to determine the maturity level that best meets their needs, according to its circumstances and the relevant legislation.

Once the maturity level for each criterion has been determined, the organization may wish to summarize the findings by calculating an overall maturity score by principle and one for the entire organization. In developing such a score, the organization should consider the following:

- sufficiency of a simple mathematical average; if insufficient, determination of the weightings to be given to the various criteria
- documentation of the rationale for weighting each criterion for use in future benchmarking.

5 PRIVACY MATURITY MODEL REPORTING

The PMM can be used as the basis for reporting on the status of the entity's privacy program and initiatives. It provides a means of reporting status and, if assessed over time, reporting progress made.

In addition, by documenting requirements of the next-higher level on the PMM, entities can determine whether and when they should initiate new privacy projects to raise their maturity level. Further, the PMM can identify situations where the maturity level has fallen and identify opportunities and requirements for remedial action.

Privacy maturity reports can be in narrative form; a more visual form can be developed using graphs and charts to indicate the level of maturity at the principle or criterion level.

The following examples based on internal reports intended for management use graphical representations.

Figure 1 – Privacy Maturity Report by GAPP Principle

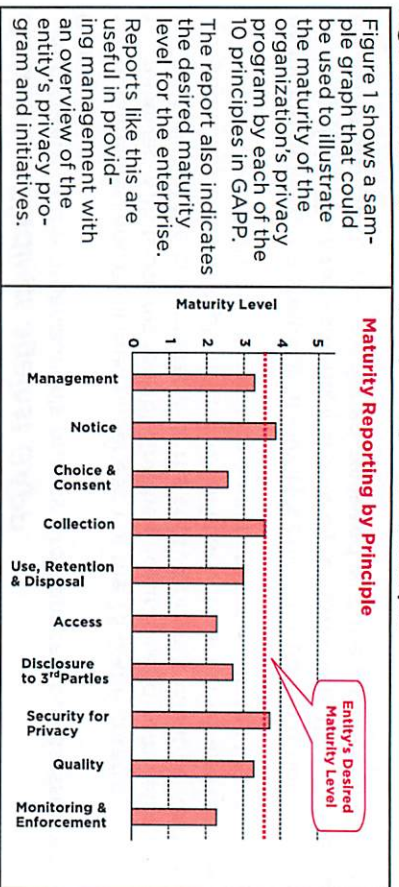


Figure 2 – Maturity Report by Criteria within a Specific GAPP Principle

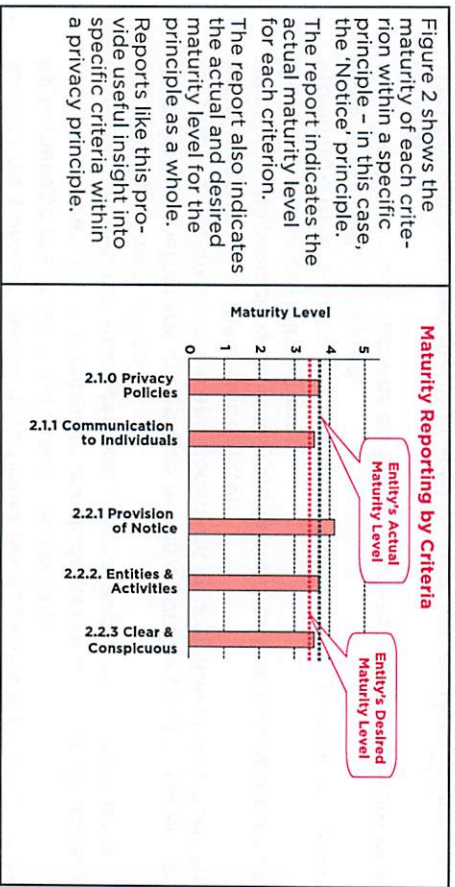
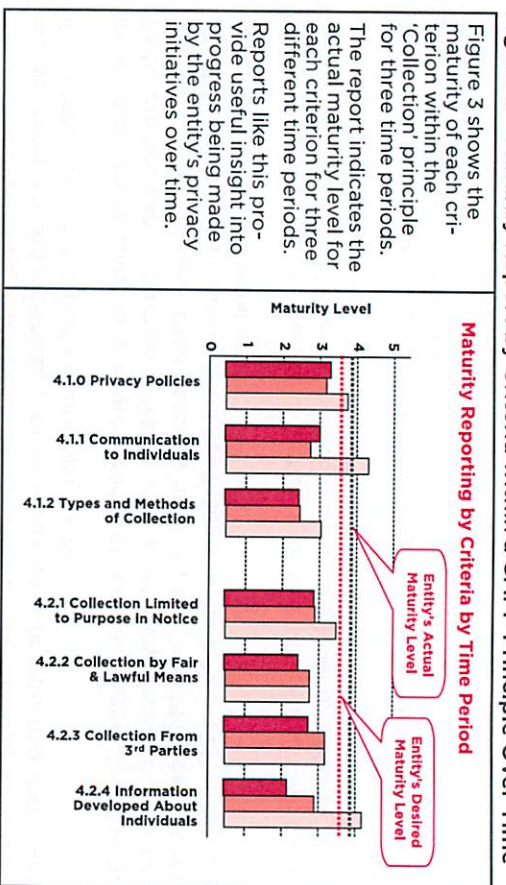


Figure 3 – Maturity Report by Criteria within a GAPP Principle Over Time



6 SUMMARY

The AICPA/CICA Privacy Maturity Model provides entities with an opportunity to assess their privacy initiatives against criteria that reflect the maturity of their privacy program and their level of compliance with Generally Accepted Privacy Principles.

The PMM can be a useful tool for management, consultants and auditors and should be considered throughout the entity's journey to develop a strong privacy program and benchmark its progress.

AICPA/CICA PRIVACY MATURITY MODEL¹

Based on Generally Accepted Privacy Principles (GAPP)²

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria)	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Policies (1.1.0)	The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	Some aspects of privacy policies exist informally.	Privacy policies exist but may not be complete, and are not fully documented.	Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.	Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Internal Personnel (1.1.1)	Privacy policies and the consequences of non-compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented.	Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete.	The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program.	Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved.

¹ This model is based on Technical Report, CMU/SEI-93TR-024 ESC-TR-93-177, "Capability Maturity Model SM for Software, Version 1.1," Copyright 1993 Carnegie Mellon University, with special permission from the Software Engineering Institute. Any material of Carnegie Mellon University and/or its Software Engineering Institute contained herein is furnished on an "as-is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement. This model has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute. © Capability Maturity Model, CMM, and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

² Published by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA)

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Responsibility and Accountability for Policies (1.1.2)	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	Management is becoming aware of privacy issues but has not yet identified a key sponsor or assigned responsibility. Privacy issues are addressed reactively.	Management understands the risks, requirements (including legal, regulatory and industry) and their responsibilities with respect to privacy. There is an understanding that appropriate privacy management is important and needs to be considered. Responsibility for operation of the entity's privacy program is assigned; however, the approaches are often informal and fragmented with limited authority or resources allocated.	Defined roles and responsibilities have been developed and assigned to various individuals / groups within the entity and employees are aware of those assignments. The approach to developing privacy policies and procedures is formalized and documented.	Management monitors the assignment of roles and responsibilities to ensure they are being performed, that the appropriate information and materials are developed and that those responsible are communicating effectively. Privacy initiatives have senior management support.	The entity (such as a committee of the board of directors) regularly monitors the processes and assignments of those responsible for privacy and analyzes the progress to determine its effectiveness. Where required, changes and improvements are made in a timely and effective fashion.
Review and Approval (1.2.1)	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Reviews are informal and not undertaken on a consistent basis.	Management undertakes periodic review of privacy policies and procedures; however, little guidance has been developed for such reviews.	Management follows a defined process that requires their review and approval of privacy policies and procedures.	The entity has supplemented management review and approval with periodic reviews by both internal and external privacy specialists.	Management's review and approval of privacy policies also include periodic assessments of the privacy program to ensure all changes are warranted, made and approved; if necessary, the approval process will be revised.
Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Reviews and comparisons with applicable laws and regulations are performed inconsistently and are incomplete.	Privacy policies and procedures have been reviewed to ensure their compliance with applicable laws and regulations; however, documented guidance is not provided.	A process has been implemented that requires privacy policies to be periodically reviewed and maintained to reflect changes in privacy legislation and regulations; however, there is no proactive review of legislation.	Changes to privacy legislation and regulations are reviewed by management and changes are made to the entity's privacy policies and procedures as required. Management may subscribe to a privacy service that regularly informs them of such changes.	Management assesses the degree to which changes to legislation are reflected in their privacy policies.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Personal Information Identification and Classification (1.2.3)	The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures.	The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information.	Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information.	All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.	All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification.	Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification.
Risk Assessment (1.2.4)	A risk assessment process is used to establish a risk baseline and, at least annually, to identify new or changed risks to personal information and to develop and update responses to such risks.	Privacy risks may have been identified, but such identification is not the result of any formal process. The privacy risks identified are incomplete and inconsistent. A privacy risk assessment has not likely been completed and privacy risks not formally documented.	Employees are aware of and consider various privacy risks. Risk assessments may not be conducted regularly, are not part of a more thorough risk management program and may not cover all areas.	Processes have been implemented for risk identification, risk assessment and reporting. A documented framework is used and risk appetite is established. For risk assessment, organizations may wish to use the AICPA/CICA Privacy Risk Assessment Tool.	Privacy risks are reviewed annually both internally and externally. Changes to privacy policies and procedures and the privacy program are updated as necessary.	The entity has a formal risk management program that includes privacy risks which may be customized by jurisdiction, business unit or function. The program maintains a risk log that is periodically assessed. A formal annual risk management review is undertaken to assess the effectiveness of the program and changes are made where necessary. A risk management plan has been implemented.
Consistency of Commitments with Privacy Policies and Procedures (1.2.5)	Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.	Reviews of contracts for privacy considerations are incomplete and inconsistent.	Procedures exist to review contracts and other commitments for instances where personal information may be involved; however, such reviews are informal and not consistently used.	A log of contracts exists and all contracts are reviewed for privacy considerations and concerns prior to execution.	Existing contracts are reviewed upon renewal to ensure continued compliance with the privacy policies and procedures. Changes in the entity's privacy policies will trigger a review of existing contracts for compliance.	Contracts are reviewed on a regular basis and tracked. An automated process has been set up to flag which contracts require immediate review when changes to privacy policies and procedures are implemented.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Infrastructure and Systems Management (1.2.6)	<p>The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:</p> <ul style="list-style-type: none"> • Infrastructure • Systems • Applications • Web sites • Procedures • Products and services • Data bases and information repositories • Mobile computing and other similar electronic devices <p>The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.</p>	Changes to existing processes or the implementation of new business and system processes for privacy issues is not consistently assessed.	Privacy impact is considered during changes to business processes and/or supporting application systems; however, these processes are not fully documented and the procedures are informal and inconsistently applied.	The entity has implemented formal procedures to assess the privacy impact of new and significantly changed products, services, business processes and infrastructure (sometimes referred to as a privacy impact assessment). The entity uses a documented systems development and change management process for all information systems and related technology employed to collect, use, retain, disclose and destroy personal information.	Management monitors and reviews compliance with policies and procedures that require a privacy impact assessment.	Through quality reviews and other independent assessments, management is informed of the effectiveness of the process for considering privacy requirements in all new and modified processes and systems. Such information is analyzed and, where necessary, changes made.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Privacy Incident and Breach Management (1.2.7)	<p>A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> • Procedures for the identification, management and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholder breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate • A process for periodic review (at least annually) of actual incidents to identify necessary program updates based on the following: <ul style="list-style-type: none"> — Incident patterns and root cause — Changes in the internal control environment or external requirements (regulation or legislation) • Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed 	Few procedures exist to identify and manage privacy incidents; however, they are not documented and are applied inconsistently.	Procedures have been developed on how to deal with a privacy incident; however, they are not comprehensive and/or inadequate employee training has increased the likelihood of unstructured and inconsistent responses.	A documented breach management plan has been implemented that includes: accountability, identification, risk assessment, response, containment, communications (including possible notification to affected individuals and appropriate authorities, if required or deemed necessary), remediation (including post-breach analysis of the breach response) and resumption.	A walkthrough of the breach management plan is performed periodically and updates to the program are made as needed.	The internal and external privacy environments are monitored for issues affecting breach risk and breach response, evaluated and improvements are made. Management assessments are provided after any privacy breach and analyzed; changes and improvements are made.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Supporting Resources (1.2.8)	Resources are provided by the entity to implement and support its privacy policies.	Resources are only allocated on an "as needed" basis to address privacy issues as they arise.	Privacy procedures exist; however, they have been "developed" within small units or groups without support from privacy specialists.	Individuals with responsibility and/or accountability for privacy are empowered with appropriate authority and resources. Such resources are made available throughout the entity.	Management ensures that adequately qualified privacy resources are identified and made available throughout the entity to support its various privacy initiatives.	Management annually reviews its privacy program and seeks ways to improve the program's performance, including assessing the adequacy, availability and performance of resources.
Qualifications of Internal Personnel (1.2.9)	The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received the necessary training.	The entity has not formally established qualifications for personnel who collect, use, disclose or otherwise handle personal information.	The entity has some established qualifications for personnel who collect, disclose, use or otherwise handle personal information, but are not fully documented. Employees receive some training on how to deal with personal information.	The entity defines qualifications for personnel who perform or manage the entity's collection, use and disclosure of personal information. Persons responsible for the protection and security of personal information have received appropriate training and have the necessary knowledge to manage the entity's collection, use and disclosure of personal information.	The entity has formed a nucleus of privacy-qualified individuals to provide privacy support to assist with specific issues, including training and job assistance.	The entity annually assesses the performance of their privacy program, including the performance and qualifications of their privacy-designated specialists. An analysis is performed of the results and changes or improvements made, as required.
Privacy Awareness and Training (1.2.10)	A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.	Formal privacy training is not provided to employees; however some knowledge of privacy may be obtained from other employees or anecdotal sources.	The entity has a privacy awareness program, but training is sporadic and inconsistent.	Personnel who handle personal information have received appropriate privacy awareness and training to ensure the entity meets obligations in its privacy notice and applicable laws. Training is scheduled, timely and consistent.	An enterprise-wide privacy awareness and training program exists and is monitored by management to ensure compliance with specific training requirements. The entity has determined which employees require privacy training and tracks their participation during such training.	A strong privacy culture exists. Compulsory privacy awareness and training is provided. Such training requires employees to complete assignments to validate their understanding. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum is made in a timely fashion.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Changes in Regulatory and Business Requirements (1.2.11)	<p>For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:</p> <ul style="list-style-type: none"> — Legal and regulatory — Contracts, including service-level agreements — Industry requirements — Business operations and processes — People, roles, and responsibilities — Technology <p>Privacy policies and procedures are updated to reflect changes in requirements.</p>	Changes in business and regulatory environments are addressed sporadically in any privacy initiatives the entity may contemplate. Any privacy-related issues or concerns that are identified only occur in an informal manner.	The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented.	The entity has implemented policies and procedures designed to monitor and act upon changes in the business and/or regulatory environment. The procedures are inclusive and employees receive training in their use as part of an enterprise-wide privacy program.	The entity has established a process to monitor the privacy environment and identify items that may impact its privacy program. Changes are considered in terms of the entity's legal, contracting, business, human resources and technology.	The entity has established a process to continually monitor and update any privacy obligations that may arise from changes to legislation, regulations, industry-specific requirements and business practices.
NOTICE (5 criteria)	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.					
Privacy Policies (2.1.0)	The entity's privacy policies address providing notice to individuals.	Notice policies and procedures exist informally.	Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented.	Notice provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (2.1.1)	<p>Notice is provided to individuals regarding the following privacy policies: purpose; choice/consent; collection; use/retention/disposal; access; disclosure to third parties; security for privacy; quality; and monitoring/enforcement.</p> <p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>	Notice to individuals is not provided in a consistent manner and may not include all aspects of privacy, such as purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding some of the following privacy policies at or before the time of collection: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding all of the following privacy policies at or before collection and is documented: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Privacy policies describe the consequences, if any, of not providing the requested information and indicate that certain information may be developed about individuals, such as buying patterns, or collected from other sources.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
NOTICE (5 criteria) cont.	The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.					
Provision of Notice (2.2.1)	Notice is provided to the individual about the entity's privacy policies and procedures (a) at or before the time personal information is collected, or as soon as practical thereafter, (b) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (c) before personal information is used for new purposes not previously identified.	Notice may not be readily accessible nor provided on a timely basis.	Notice provided to individuals is generally accessible but is not provided on a timely basis. Notice may not be provided in all cases when personal information is collected or used for new purposes.	The privacy notice is documented, readily accessible and available, provided in a timely fashion and clearly dated.	The entity tracks previous iterations of the privacy policies and individuals are informed about changes to a previously communicated privacy notice. The privacy notice is updated to reflect changes to policies and procedures.	The entity solicits input from relevant stakeholders regarding the appropriate means of providing notice and makes changes as deemed appropriate. Notice is provided using various techniques to meet the communications technologies of their constituents (e.g. social media, mobile communications, etc).
Entities and Activities Covered (2.2.2)	An objective description of the entities and activities covered by privacy policies is included in the privacy notice.	The privacy notice may not include all relevant entities and activities.	The privacy notice describes some of the particular entities, business segments, locations, and types of information covered.	The privacy notice objectively describes and encompasses all relevant entities, business segments, locations, and types of information covered.	The entity performs a periodic review to ensure the entities and activities covered by privacy policies are updated and accurate.	Management follows a formal documented process to consider and take appropriate action as necessary to update privacy policies and the privacy notice prior to any change in the entity's business structure and activities.
Clear and Conspicuous (2.2.3)	The privacy notice is conspicuous and uses clear language.	Privacy policies are informal, not documented and may be phrased differently when orally communicated.	The privacy notice may be informally provided but is not easily understood, nor is it easy to see or easily available at points of data collection. If a formal privacy notice exists, it may not be clear and conspicuous.	The privacy notice is in plain and simple language, appropriately labeled, easy to see, and not in small print. Privacy notices provided electronically are easy to access and navigate.	Similar formats are used for different and relevant subsidiaries or segments of an entity to avoid confusion and allow consumers to identify any differences. Notice formats are periodically reviewed for clarity and consistency.	Feedback about improvements to the readability and content of the privacy policies are analyzed and incorporated into future versions of the privacy notice.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria)	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Privacy Policies (3.1.0)	The entity's privacy policies address the choices to individuals and the consent to be obtained.	Choice and consent policies and procedures exist informally.	Choice and consent provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Choice and consent provisions in privacy policies and procedures cover all relevant aspects and are fully documented.	Compliance with choice and consent provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to choice and consent. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (3.1.1)	Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.	Individuals may be informed about the choices available to them; however, communications are inconsistent, sporadic and undocumented.	The entity's privacy notice describes in a clear and concise manner some of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required.	The entity's privacy notice describes, in a clear and concise manner, all of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required.	Privacy policies and procedures are reviewed periodically to ensure the choices available to individuals are updated as necessary and the use of explicit or implicit consent is appropriate with regard to the personal information being used or disclosed.	Changes and improvements to messaging and communications techniques and technologies are made in response to periodic assessments and feedback.
Consequences of Denying or Withdrawing Consent (3.1.2)	When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.	Individuals may not be informed consistently about the consequences of refusing, denying or withdrawing.	Consequences may be identified but may not be fully documented or consistently disclosed to individuals.	Individuals are informed about the consequences of refusing to provide personal information or denying or withdrawing consent.	Processes are in place to review the stated consequences periodically to ensure completeness, accuracy and relevance.	Processes are implemented to reduce the consequences of denying consent, such as increasing the granularity of the application of such consequences.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria) cont.	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Implicit or Explicit Consent (3.2.1)	Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.	Consent is neither documented nor consistently obtained at or before collection of personal information.	Consent is consistently obtained, but may not be documented or obtained in a timely fashion.	Consent is obtained before or at the time personal information is collected and preferences are implemented (such as making appropriate database changes and ensuring that programs that access the database test for the preference). Explicit consent is documented and implicit consent processes are appropriate. Processes are in place to ensure that consent is recorded by the entity and referenced prior to future use.	An individual's preferences are confirmed and any changes are documented and referenced prior to future use.	Consent processes are periodically reviewed to ensure the individual's preferences are being appropriately recorded and acted upon and, where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.
Consent for New Purposes and Uses (3.2.2)	If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and implicit or explicit consent is obtained prior to such new use or purpose.	Individuals are not consistently notified about new proposed uses of personal information previously collected.	Individuals are consistently notified about new purposes not previously specified. A process exists to notify individuals but may not be fully documented and consent might not be obtained before new uses.	Consent is obtained and documented prior to using personal information for purposes other than those for which it was originally collected.	Processes are in place to ensure personal information is used only in accordance with the purposes for which consent has been obtained and to ensure it is not used if consent is withdrawn. Monitoring is in place to ensure personal information is not used without proper consent.	Consent processes are periodically reviewed to ensure consent for new purposes is being appropriately recorded and acted upon and where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.
Explicit Consent for Sensitive Information (3.2.3)	Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.	Explicit consent is not consistently obtained prior to collection of sensitive personal information.	Employees who collect personal information are aware that explicit consent is required when obtaining sensitive personal information; however, the process is not well defined or fully documented.	A documented formal process has been implemented requiring explicit consent be obtained directly from the individual prior to, or as soon as practically possible, after collection of sensitive personal information.	The process is reviewed and compliance monitored to ensure explicit consent is obtained prior to, or as soon as practically possible, after collection of sensitive personal information.	For procedures that collect sensitive personal information and do not obtain explicit consent, remediation plans are identified and implemented to ensure explicit consent has been obtained.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
CHOICE and CONSENT (7 criteria) cont.	The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.					
Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices (3.2.4)	Consent is obtained before personal information is transferred to/from an individual's computer or similar device.	Consent is not consistently obtained before personal information is transferred to/from another computer or other similar device.	Software enables an individual to provide consent before personal information is transferred to/from another computer or other similar device.	The application is designed to consistently solicit and obtain consent before personal information is transferred to/from another computer or other similar device and does not make any such transfers if consent has not been obtained. Such consent is documented.	The process is reviewed and compliance monitored to ensure consent is obtained before any personal information is transferred to/from an individual's computer or other similar device.	Where procedures have been identified that do not obtain consent before personal information is transferred to/from an individual's computer or other similar device, remediation plans are identified and implemented.
COLLECTION (7 criteria)	The entity collects personal information only for the purposes identified in the notice.					
Privacy Policies (4.1.0)	The entity's privacy policies address the collection of personal information.	Collection policies and procedures exist informally.	Collection provisions in privacy policies and procedures exist but might not cover all aspects, and are not fully documented.	Collection provisions in privacy policies cover all relevant aspects of collection and are fully documented.	Compliance with collection provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to collection. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (4.1.1)	Individuals are informed that personal information is collected only for the purposes identified in the notice.	Individuals may be informed that personal information is collected only for purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed that personal information is collected only for the purposes identified in the notice. Such notification is generally not documented.	Individuals are informed that personal information is collected only for the purposes identified in the notice and the sources and methods used to collect this personal information are identified. Such notification is available in written format.	Privacy policies are reviewed periodically to ensure the areas related to collection are updated as necessary.	Changes and improvements to messaging and communications methods and techniques are made in response to periodic assessments and feedback.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
COLLECTION (7 criteria) cont.	The entity collects personal information only for the purposes identified in the notice.					
Types of Personal Information Collected and Methods of Collection (4.1.2)	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.	Individuals may be informed about the types of personal information collected and the methods of collection; however, communications are informal, may not be complete and may not fully describe the methods of collection.	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are neither fully documented nor fully described in the privacy notice.	The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are fully documented and fully described in the privacy notice. The notice also discloses whether information is developed or acquired about individuals, such as buying patterns. The notice also describes the consequences if the cookie is refused.	Management monitors business processes to identify new types of personal information collected and new methods of collection to ensure they are described in the privacy notice.	The privacy notice is reviewed regularly and updated in a timely fashion to describe all the types of personal information being collected and the methods used to collect them.
Collection Limited to Identified Purpose (4.2.1)	The collection of personal information is limited to that necessary for the purposes identified in the notice.	Informal and undocumented procedures are relied upon to ensure collection is limited to that necessary for the purposes identified in the privacy notice.	Policies and procedures, may not: <ul style="list-style-type: none"> • be fully documented; • distinguish the personal information essential for the purposes identified in the notice; • differentiate personal information from optional information. 	Policies and procedures that have been implemented are fully documented to clearly distinguish the personal information essential for the purposes identified in the notice and differentiate it from optional information. Collection of personal information is limited to information necessary for the purposes identified in the privacy notice.	Policies and procedures are in place to periodically review the entity's needs for personal information.	Policies, procedures and business processes are updated due to changes in the entity's needs for personal information. Corrective action is undertaken when information not necessary for the purposes identified is collected.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
COLLECTION (7 criteria) cont.	The entity collects personal information only for the purposes identified in the notice.					
Collection by Fair and Lawful Means (4.2.2)	Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	Informal procedures exist limiting the collection of personal information to that which is fair and lawful; however, they may be incomplete and inconsistently applied.	Management may conduct reviews of how personal information is collected, but such reviews are inconsistent and untimely. Policies and procedures related to the collection of personal information are either not fully documented or incomplete.	Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	Methods of collecting personal information are periodically reviewed by management after implementation to confirm personal information is obtained fairly and lawfully.	Complaints to the entity are reviewed to identify where unlawful or deceptive practices exist. Such complaints are reviewed, analyzed and changes to policies and procedures to correct such practices are implemented.
Collection from Third Parties (4.2.3)	Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.	Limited guidance and direction exist to assist in the review of third-party practices regarding collection of personal information.	Reviews of third-party practices are performed but such procedures are not fully documented.	The entity consistently reviews privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources. Clauses are included in agreements that require third-parties to collect information fairly and lawfully and in accordance with the entity's privacy policies.	Once agreements have been implemented, the entity conducts a periodic review of third-party collection of personal information. Corrective actions are discussed with third parties.	Lessons learned from contracting and contract management processes are analyzed and, where appropriate, improvements are made to existing and future contracts involving collection of personal information involving third parties.
Information Developed About Individuals (4.2.4)	Individuals are informed if the entity develops or acquires additional information about them for its use.	Policies and procedures informing individuals that additional information about them is being collected or used are informal, inconsistent and incomplete.	Policies and procedures exist to inform individuals when the entity develops or acquires additional personal information about them for its use; however, procedures are not fully documented or consistently applied.	The entity's privacy notice indicates that, if applicable, it may develop and/or acquire information about individuals by using third-party sources, browsing, e-mail content, credit and purchasing history. Additional consent is obtained where necessary.	The entity monitors information collection processes, including the collection of additional information, to ensure appropriate notification and consent requirements are complied with. Where necessary, changes are implemented.	The entity's privacy notice provides transparency in the collection, use and disclosure of personal information. Individuals are given multiple opportunities to learn how personal information is developed or acquired.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
USE, RETENTION AND DISPOSAL (5 criteria)	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.					
Privacy Policies (5.1.0)	The entity's privacy policies address the use, retention, and disposal of personal information.	Procedures for the use, retention and disposal of personal information are ad hoc, informal and likely incomplete.	Use, retention and disposal provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Use, retention and disposal provisions in privacy policies and procedures cover all relevant aspects and are fully documented.	Compliance with use, retention and disposal provisions in privacy policies and procedures is monitored.	Management monitors compliance with privacy policies and procedures relating to use, retention and disposal. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.
Communication to Individuals (5.1.1)	Individuals are informed that personal information is (a) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (b) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse or unauthorized access.	Individuals may be informed about the uses, retention and disposal of their personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed about the use, retention and disposal of personal information, but this communication may not cover all aspects and is not fully documented. Retention periods are not uniformly communicated.	Individuals are consistently and uniformly informed about use, retention and disposal of personal information. Data retention periods are identified and communicated to individuals.	Methods are in place to update communications when changes occur to use, retention and disposal practices.	Individuals' general level of understanding of use, retention and disposal of personal information is assessed. Feedback is used to continuously improve communication methods.
Use of Personal Information (5.2.1)	Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	The use of personal information may be inconsistent with the purposes identified in the notice. Consent is not always obtained consistently.	Policies and procedures regarding the use of information have been adopted; however, they are not documented and may not be consistently applied.	Use of personal information is consistent with the purposes identified in the privacy notice. Consent for these uses is consistently obtained. Uses of personal information throughout the entity are in accordance with the individual's preferences and consent.	Uses of personal information are monitored and periodically reviewed for appropriateness. Management ensures that any discrepancies are corrected on a timely basis.	The uses of personal information are monitored and periodically assessed for appropriateness; verifications of consent and usage are conducted through the use of automation. Any discrepancies are remediated in a timely fashion. Changes to laws and regulations are monitored and the entity's policies and procedures are amended as required.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
USE, RETENTION AND DISPOSAL (5 criteria) cont.	The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.					
Retention of Personal Information (5.2.2)	Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.	The retention of personal information is irregular and inconsistent.	Policies and procedures for identifying retention periods of personal information have been adopted, but may not be fully documented or cover all relevant aspects.	The entity has documented its retention policies and procedures and consistently retains personal information in accordance with such policies and practices.	Retention practices are periodically reviewed for compliance with policies and changes implemented when necessary.	The retention of personal information is monitored and periodically assessed for appropriateness, and verifications of retention are conducted. Such processes are automated to the extent possible. Any discrepancies found are remediated in a timely fashion.
Disposal, Destruction and Redaction of Personal Information (5.2.3)	Personal information no longer retained is anonymized, disposed of or destroyed in a manner that prevents loss, theft, misuse or unauthorized access.	The disposal, destruction and redaction of personal information is irregular, inconsistent and incomplete.	Policies and procedures for identifying appropriate and current processes and techniques for the appropriate disposal, destruction and redaction of personal information have been adopted but are not fully documented or complete.	The entity has documented its policies and procedures regarding the disposal, destruction and redaction of personal information, implemented such practices and ensures that these practices are consistent with the privacy notice.	The disposal, destruction, and redaction of personal information are consistently documented and periodically reviewed for compliance with policies and appropriateness.	The disposal, destruction, and redaction of personal information are monitored and periodically assessed for appropriateness, and verification of the disposal, destruction and redaction conducted. Such processes are automated to the extent possible. Any discrepancies found are remediated in a timely fashion.
ACCESS (8 criteria)	The entity provides individuals with access to their personal information for review and update.					
Privacy Policies (6.1.0)	The entity's privacy policies address providing individuals with access to their personal information.	Informal access policies and procedures exist.	Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Compliance with access provisions in privacy policies and procedures is monitored.	Management monitors compliance with privacy policies and procedures relating to access. Issues of non-compliance are identified and remedial action taken to ensure compliance.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Communication to Individuals (6.1.1)	Individuals are informed about how they may obtain access to their personal information to review, update and correct that information.	Individuals may be informed about how they may obtain access to their personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated.	Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated.	Processes are in place to update communications to individuals when changes occur to access policies, procedures and practices.	The entity ensures that individuals are informed about their personal information access rights, including update and correction options, through channels such as direct communication programs, notification on statements and other mailings and training and awareness programs for staff. Management monitors and assesses the effects of its various initiatives and seeks to continuously improve methods of communication and understanding.
Access by Individuals to their Personal Information (6.2.1)	Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.	The entity has informal procedures granting individuals access to their information; however, such procedures are not documented and may not be consistently applied.	Some procedures are in place to allow individuals to access their personal information, but they may not cover all aspects and may not be fully documented.	Procedures to search for an individual's personal information and to grant individuals access to their information have been documented, implemented and cover all relevant aspects. Employees have been trained in how to respond to these requests, including recording such requests.	Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided. The entity identifies and implements measures to improve the efficiency of its searches for an individual's personal information.	The entity reviews the processes used to handle access requests to determine where improvements may be made and implements such improvements. Access to personal information is automated and self-service when possible and appropriate.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Confirmation of an Individual's Identity (6.2.2)	The identity of individuals who request access to their personal information is authenticated before they are given access to that information.	Procedures to authenticate individuals requesting access to their information are informal, not documented and may not be consistently applied.	Procedures are in place to confirm the identity of individuals requesting access to their personal information before they are granted access, but do not cover all aspects and may not be documented. Level of authentication required may not be appropriate to the personal information being accessed.	Confirmation/authentication methods have been implemented to uniformly and consistently confirm the identity of individuals requesting access to their personal information, including the training of employees.	Procedures are in place to track and monitor the confirmation/authentication of individuals before they are granted access to personal information, and to review the validity of granting access to such personal information.	The successful confirmation/authentication of individuals before they are granted access to personal information is monitored and periodically assessed for type 1 (where errors are not caught) and type 2 (where an error has been incorrectly identified) errors. Remediation plans to lower the error rates are formulated and implemented.
Understandable Personal Information, Time Frame, and Cost (6.2.3)	Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.	The entity has some informal procedures designed to provide information to individuals in an understandable form. Timeframes and costs charged may be inconsistent and unreasonable.	Procedures are in place requiring that personal information be provided to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost, but may not be fully documented or cover all aspects.	Procedures have been implemented that consistently and uniformly provide personal information to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost.	Procedures are in place to track and monitor the response time in providing personal information, the associated costs incurred by the entity and any charges to the individual making the request. Periodic assessments of the understandability of the format for information provided to individuals are conducted.	Reports of response times in providing personal information are monitored and assessed. The associated costs incurred by the entity and any charges to the individual making the request are periodically assessed. Periodic assessments of the understandability of the format for information provided to individuals are conducted. Remediation plans are made and implemented for unacceptable response time, excessive or inconsistent charges and difficult-to-read personal information report formats. Conversion of personal information to an understandable form is automated where possible and appropriate.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Denial of Access (6.2.4)	Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.	Informal procedures are used to inform individuals, of the reason a request for access to their personal information was denied; however they are incomplete and inconsistently applied.	Procedures are in place to inform individuals of the reason a request for access to their personal information was denied, but they may not be documented or cover all aspects. Notification may not be in writing or include the entity's legal rights to deny such access and the individual's right to challenge denials.	Consistently applied and uniform procedures have been implemented to inform individuals in writing of the reason a request for access to their personal information was denied. The entity's legal rights to deny such access have been identified as well as the individual's right to challenge denials.	Procedures are in place to review the response time to individuals whose access request has been denied, reasons for such denials, as well as any communications regarding challenges.	Reports of denial reasons, response times and challenge communications are monitored and assessed. Remediation plans are identified and implemented for unacceptable response time and inappropriate denials of access. The denial process is automated and includes electronic responses where possible and appropriate.
Updating or Correcting Personal Information (6.2.5)	Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information.	Informal and undocumented procedures exist that provide individuals with information on how to update or correct personal information held by the entity; however, they are incomplete and inconsistently applied.	Some procedures are in place for individuals to update or correct personal information held by the entity, but they are not complete and may not be fully documented. A process exists to review and confirm the validity of such requests and inform third parties of changes made; however, not all of the processes are documented.	Documented policies with supporting procedures have been implemented to consistently and uniformly inform individuals of how to update or correct personal information held by the entity. Procedures have been implemented to consistently and uniformly provide updated information to third parties that previously received the individual's personal information.	Procedures are in place to track data update and correction requests and to validate the accuracy and completeness of such data. Documentation or justification is kept for not providing information updates to relevant third parties.	Reports of updates and correction requests and response time to update records are monitored and assessed. Documentation or justification for not providing information updates to relevant third parties is monitored and assessed to determine whether the economically feasible requirement was met. Updating is automated and self-service where possible and appropriate. Distribution of updated information to third parties is also automated where possible and appropriate.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
ACCESS (8 criteria) cont.	The entity provides individuals with access to their personal information for review and update.					
Statement of Disagreement (6.2.6)	Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.	Procedures used to inform individuals of the reason a request for correction of personal information was denied, and how they may appeal are inconsistent and undocumented.	Procedures are in place to inform individuals about the reason a request for correction of personal information was denied, and how they may appeal, but they are not complete or documented.	Documented policies and procedures that cover relevant aspects have been implemented to inform individuals in writing about the reason a request for correction of personal information was denied, and how they may appeal.	Procedures are in place to track and review the reasons a request for correction of personal information was denied.	Cases that involve disagreements over the accuracy and completeness of personal information are reviewed and remediation plans are identified and implemented as appropriate. The process to complete a Statement of Disagreement is automated where possible and appropriate.
DISCLOSURE TO THIRD PARTIES (7 criteria)	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Privacy Policies (7.1.0)	The entity's privacy policies address the disclosure of personal information to third parties.	Informal disclosure policies and procedures exist but may not be consistently applied.	Disclosure provisions in privacy policies exist but may not cover all aspects, and are not fully documented.	Disclosure provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with disclosure provisions in privacy policies is monitored.	Management monitors compliance with privacy policies and procedures relating to disclosure to third parties. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (7.1.1)	Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise.	Individuals may be informed that personal information is disclosed to third parties only for the purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented.	Procedures are in place to inform individuals that personal information is disclosed to third parties; however, limited documentation exists and the procedures may not be performed consistently or in accordance with relevant laws and regulations.	Documented procedures that cover all relevant aspects, and in accordance with relevant laws and regulations are in place to inform individuals that personal information is disclosed to third parties, but only for the purposes identified in the privacy notice and for which the individual has provided consent. Third parties or classes of third parties to whom personal information is disclosed are identified.	Procedures exist to review new or changed business processes, third parties or regulatory bodies requiring compliance to ensure appropriate communications to individuals are provided and consent obtained where necessary.	Issues identified or communicated to the entity with respect to the disclosure of personal information to third parties are monitored and, where necessary, changes and improvements made to the policies and procedures to better inform individuals.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Communication to Third Parties (7.1.2)	Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.	Procedures to communicate to third parties their responsibilities with respect to personal information provided to them are informal, inconsistent and incomplete.	Procedures are in place to communicate to third parties the entity's privacy policies or other specific instructions or requirements for handling personal information, but they are inconsistently applied and not fully documented.	Documented policies and procedures exist and are consistently and uniformly applied to communicate to third parties the privacy policies or other specific instructions or requirements for handling personal information. Written agreements with third parties are in place confirming their adherence to the entity's privacy policies and procedures.	A review is periodically performed to ensure third parties have received the entity's privacy policies, instructions and other requirements relating to personal information that has been disclosed. Acknowledgement of the receipt of the above is monitored.	Contracts and other agreements involving personal information provided to third parties are reviewed to ensure the appropriate information has been communicated and agreement has been obtained. Remediation plans are developed and implemented where required.
Disclosure of Personal Information (7.2.1)	Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise.	Procedures regarding the disclosure of personal information to third parties are informal, incomplete and applied inconsistently.	Procedures are in place to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise; however, such procedures may not be fully documented or consistently and uniformly evaluated.	Documented procedures covering all relevant aspects have been implemented to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise. They are uniformly and consistently applied.	Procedures are in place to test and review whether disclosure to third parties is in compliance with the entity's privacy policies.	Reports of personal information provided to third parties are maintained and such reports are reviewed to ensure only information that has consent has been provided to third parties. Remediation plans are developed and implemented where inappropriate disclosure has occurred or where third parties are not in compliance with their commitments. Disclosure to third parties may be automated.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Protection of Personal Information (7.2.2)	Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	Procedures used to ensure third-party agreements are in place to protect personal information prior to disclosing to third parties are informal, incomplete and inconsistently applied. The entity does not have procedures to evaluate the effectiveness of third-party controls to protect personal information.	Procedures are in place to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements, but are not consistently and uniformly applied or fully documented. Some procedures are in place to determine whether third parties have reasonable controls; however, they are not consistently and uniformly assessed.	Documented policies and procedures covering all relevant aspects have been implemented to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures to evaluate whether third parties have effective controls to meet the terms of the agreement, instructions or requirements.	An assessment of third party procedures is periodically performed to ensure such procedures continue to meet the entity's requirements. Such assessments may be performed by the entity or an independent qualified third party.	Changes in a third-party environment are monitored to ensure the third party can continue to meet its obligations with respect to personal information disclosed to them. Remediation plans are developed and implemented where necessary. The entity evaluates compliance using a number of approaches to obtain an increasing level of assurance depending on its risk assessment.
New Purposes and Uses (7.2.3)	Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.	Procedures to ensure the proper disclosure of personal information to third parties for new purposes or uses are informal, inconsistent and incomplete.	Procedures exist to ensure the proper disclosure of personal information to third parties for new purposes; however, they may not be consistently and uniformly applied and not fully documented.	Documented procedures covering all relevant aspects have been implemented to ensure the proper disclosure of personal information to third parties for new purposes. Such procedures are uniformly and consistently applied. Consent from individuals prior to disclosure is documented. Existing agreements with third parties are reviewed and updated to reflect the new purposes and uses.	Monitoring procedures are in place to ensure proper disclosure of personal information to third parties for new purposes. The entity monitors to ensure the newly disclosed information is only being used for the new purposes or as specified.	Reports of disclosure of personal information to third parties for new purposes and uses, as well as the associated consent by the individual, where applicable, are monitored and assessed, to ensure appropriate consent has been obtained and documented. Collection of consent for new purposes and uses is automated where possible and appropriate.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
DISCLOSURE TO THIRD PARTIES (7 criteria) cont.	The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.					
Misuse of Personal Information by a Third Party (7.2.4)	The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.	Procedures to determine and address misuse of personal information by a third party are informal, incomplete and inconsistently applied.	Procedures are in place to require remedial action in response to misuse of personal information by a third party, but they are not consistently and uniformly applied or fully documented.	Documented policies and procedures covering all relevant aspects are in place to take remedial action in response to misuse of personal information by a third party. Such procedures are consistently and uniformly applied.	Monitoring procedures are in place to track the response to misuse of personal information by a third party from initial discovery through to remedial action.	Exception reports are used to record inappropriate or unacceptable activities by third parties and to monitor the status of remedial activities. Remediation plans are developed and procedures implemented to address unacceptable or inappropriate use.
SECURITY FOR PRIVACY (9 criteria)	The entity protects personal information against unauthorized access (both physical and logical).					
Privacy Policies (8.1.0)	The entity's privacy policies (including any relevant security policies) address the security of personal information.	Security policies and procedures exist informally; however, they are based on ad hoc and inconsistent processes.	Security provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Security provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with security provisions in privacy policies and procedures is evaluated and monitored.	Management monitors compliance with privacy policies and procedures relating to security. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (8.1.1)	Individuals are informed that precautions are taken to protect personal information.	Individuals may be informed about security of personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed about security practices to protect personal information, but such disclosures may not cover all aspects and are not fully documented.	Individuals are informed about the entity's security practices for the protection of personal information. Security policies, procedures and practices are documented and implemented.	The entity manages its security program through periodic reviews and security assessments. Incidents and violations of its communications policy for security are investigated.	Communications explain to individuals the need for security, the initiatives the entity takes to ensure that personal information is protected and informs individuals of other activities they may want to take to further protect their information.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Information Security Program (8.2.1)	<p>A security program has been developed, documented, approved, and implemented that includes administrative, technical and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The security program should address, but not be limited to, the following areas³ insofar as they relate to the security of personal information:</p> <ul style="list-style-type: none"> a. Risk assessment and treatment [1.2.4] b. Security policy [8.1.0] c. Organization of information security [sections 1, 7, and 10] d. Asset management [section 1] e. Human resources security [section 1] f. Physical and environmental security [8.2.3 and 8.2.4] g. Communications and operations management [sections 1, 7, and 10] h. Access control [sections 1, 8.2, and 10] i. Information systems acquisition, development, and maintenance [1.2.6] j. Information security incident management [1.2.7] k. Business continuity management [section 8.2] l. Compliance [sections 1 and 10] 	There have been some thoughts of a privacy-focused security program, but limited in scope and perhaps undocumented.	The entity has a security program in place that may not address all areas or be fully documented.	<p>The entity has developed, documented and promulgated its comprehensive enterprise-wide security program.</p> <p>The entity has addressed specific privacy-focused security requirements.</p>	Management monitors weaknesses, periodically reviews its security program as it applies to personal information and establishes performance benchmarks.	The entity undertakes annual reviews of its security program, including external reviews, and determines the effectiveness of its procedures. The results of such reviews are used to update and improve the security program.

³ These areas are drawn from ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management. Permission is granted by the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). Copies of ISO/IEC 27002 can be purchased from ANSI in the United States at <http://webstore.ansi.org/> and in Canada from the Standards Council of Canada at www.standardsstore.ca/eSpecs/index.jsp. It is not necessary to meet all of the criteria of ISO/IEC 27002:2005 to satisfy Generally Accepted Privacy Principles' criterion 8.2.1. The references associated with each area indicate the most relevant Generally Accepted Privacy Principles' criteria for this purpose.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Logical Access Controls (8.2.2)	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> a. Authorizing and registering internal personnel and individuals b. Identifying and authenticating internal personnel and individuals c. Making changes and updating access profiles d. Granting privileges and permissions for access to IT infrastructure components and personal information e. Preventing individuals from accessing anything other than their own personal or sensitive information f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities g. Distributing output only to authorized internal personnel h. Restricting logical access to offline storage, backup data, systems and media i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) j. Preventing the introduction of viruses, malicious code, and unauthorized software 	Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete.	The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information.	<p>The entity has documented and implemented security policies and procedures that sufficiently control access to personal information.</p> <p>Access to personal information is restricted to employees with a need for such access.</p>	<p>Management monitors logical access controls, including access attempts and violation reports for files, databases and resources containing personal information to identify areas where additional security needs improvement.</p> <p>Irregular access of authorized personnel is also monitored.</p>	<p>Access and violation attempts are assessed to determine root causes and potential exposures and remedial action plans are developed and implemented to increase the level of protection of personal information. Logical access controls are continually assessed and improved.</p> <p>Irregular access of authorized personnel is monitored, assessed and investigated where necessary.</p>

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Physical Access Controls (8.2.3)	Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Controls over physical access to personal information are informal, incomplete and inconsistent.	The entity has basic physical security procedures; however, they do not include specific requirements governing physical access to personal information maintained or stored in various media. Accordingly, inconsistent approaches are taken throughout the entity with respect to physically securing personal information.	The entity has implemented formal physical security policies and procedures that form the basis of specific privacy-related security procedures for physical access to personal information. Physical access to personal information is restricted to employees with a need for such access.	Management monitors physical access controls. Personal information is physically stored in secure locations. Access to such locations is restricted and monitored. Unauthorized access is investigated and appropriate action taken.	Where physical access or attempted violation of personal information has occurred, the events are analyzed and remedial action including changes to policies and procedures is adopted. This may include implementing increased use of technology, as necessary. Physical access controls are continually assessed and improved.
Environmental Safeguards (8.2.4)	Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Some policies and procedures exist to ensure adequate safeguards over personal information in the event of disasters or other environmental hazards; however, they are incomplete and inconsistently applied. The entity may lack a business continuity plan that would require an assessment of threats and vulnerabilities and appropriate protection of personal information.	The entity has a business continuity plan addressing certain aspects of the business. Such a plan may not specifically address personal information. Accordingly, personal information may not be appropriately protected. Business continuity plans are not well documented and have not been tested.	The entity has implemented a formal business-continuity and disaster-recovery plan that address all aspects of the business and identified critical and essential resources, including personal information in all forms and media, and provides for specifics thereof. Protection includes protection against accidental, unauthorized or inappropriate access or disclosure of personal information. The plan has been tested.	Management monitors threats and vulnerabilities as part of a business risk management program and, where appropriate, includes personal information as a specific category.	Management risk and vulnerability assessments with respect to personal information result in improvements to the protection of such information.
Transmitted Personal Information (8.2.5)	Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry-standard encryption technology for transferring and receiving personal information.	The protection of personal information when being transmitted or sent to another party is informal, incomplete and inconsistently applied. Security restrictions may not be applied when using different types of media to transmit personal information.	Policies and procedures exist for the protection of information during transmittal but are not fully documented; however, they may not specifically address personal information or types of media.	Documented procedures that cover all relevant aspects have been implemented and are working effectively to protect personal information when transmitted.	The entity's policies and procedures for the transmission of personal information are monitored to ensure that they meet minimum industry security standards and the entity is in compliance with such standards and their own policies and procedures. Issues of non-compliance are dealt with.	Management reviews advances in security technology and techniques and updates their security policies and procedures and supporting technologies to afford the entity the most effective protection of personal information while it is being transmitted, regardless of the media used.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Personal Information on Portable Media (8.2.6)	Personal information stored on portable media or devices is protected from unauthorized access.	Controls over portable devices that contain personal information are informal, incomplete and inconsistent.	Procedures are in place to protect personal information on portable devices; however, they are not fully documented. Employees are aware of the additional risks and vulnerabilities associated with the use of portable and removable devices. Awareness of requirements to protect personal information are known and certain procedures exist to preclude or restrict the use of portable and removal devices to record, transfer and archive personal information.	The entity has implemented documented policies and procedures, supported by technology, that cover all relevant aspects and restrict the use of portable or removable devices to store personal information. The entity authorizes the devices and requires mandatory encryption.	Prior to issuance of portable or removable devices, employees are required to read and acknowledge their responsibilities for such devices and recognize the consequences of violations of security policies and procedures. Where portable devices are used, only authorized and registered devices such as portable flash drives that require encryption are permitted. Use of unregistered and unencrypted portable devices is not allowed in the entity's computing environment.	Management monitors new technologies to enhance the security of personal information stored on portable devices. They ensure the use of new technologies meets security requirements for the protection of personal information, monitor adoption and implementation of such technologies and, where such monitoring identifies deficiencies or exposures, implement remedial action.
Testing Security Safeguards (8.2.7)	Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Tests of security safeguards for personal information are undocumented, incomplete and inconsistent.	Periodic tests of security safeguards are performed by the IT function; however, their scope varies.	Periodic and appropriate tests of security safeguards for personal information are performed in all significant areas of the business. Test work is completed by qualified personnel such as Certified Public Accountants, Chartered Accountants, Certified Information System Auditors, or internal auditors. Test results are documented and shared with appropriate stakeholders. Tests are performed at least annually.	Management monitors the testing process, ensures tests are conducted as required by policy, and takes remedial action for deficiencies identified.	Test results are analyzed, through a defined root-cause analysis, and remedial measures documented and implemented to improve the entity's security program.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
QUALITY (4 criteria)	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
Privacy Policies (9.1.0)	The entity's privacy policies address the quality of personal information.	Quality control policies and procedures exist informally.	Quality provisions in privacy policies and procedures exist, but may not cover all aspects and are not fully documented.	Quality provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with quality provisions in privacy policies and procedures is monitored and the results are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to quality. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (9.1.1)	Individuals are informed that they are responsible for providing the entity with accurate and complete personal information and for contacting the entity if correction of such information is required.	Individuals may be informed about their responsibility to provide accurate and complete personal information; however, communications are inconsistent, sporadic and undocumented.	Individuals are informed of their responsibility to provide accurate information; however, communications may not cover all aspects and may not be fully documented.	Individuals are informed of their responsibility for providing accurate and complete personal information and for contacting the entity if corrections are necessary. Such communications cover all relevant aspects and are documented.	Communications are monitored to ensure individuals are adequately informed of their responsibilities and the remedies available to them should they have complaints or issues.	Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required.
Accuracy and Completeness of Personal Information (9.2.1)	Personal information is accurate and complete for the purposes for which it is to be used.	Procedures exist to ensure the completeness and accuracy of information provided to the entity; however, they are informal, incomplete and inconsistently applied.	Procedures are in place to ensure the accuracy and completeness of personal information; however, they are not fully documented and may not cover all aspects.	Documented policies, procedures and processes that cover all relevant aspects have been implemented to ensure the accuracy of personal information. Individuals are provided with information on how to correct data the entity maintains about them.	Processes are designed and managed to ensure the integrity of personal information is maintained. Benchmarks have been established and compliance measured. Methods are used to verify the accuracy and completeness of personal information obtained, whether from individuals directly or from third parties.	Processes are in place to monitor and measure the accuracy of personal information. Results are analyzed and modifications and improvements made.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
QUALITY (4 criteria) cont.	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
Relevance of Personal Information (9.2.2)	Personal information is relevant to the purposes for which it is to be used.	Some procedures are in place to ensure the personal information being collected is relevant to the defined purpose, but they are incomplete, informal and inconsistently applied.	Procedures are in place to ensure that personal information is relevant to the purposes for which it is to be used, but these procedures are not fully documented nor cover all aspects.	Documented policies and procedures that cover all relevant aspects, supported by effective processes, have been implemented to ensure that only personal information relevant to the stated purposes is used and to minimize the possibility that inappropriate information is used to make business decisions about the individual.	Processes are designed and reviewed to ensure the relevance of the personal information collected, used and disclosed.	Processes are in place to monitor the relevance of personal information collected, used and disclosed. Results are analyzed and modifications and improvements made as necessary.
MONITORING and ENFORCEMENT (7 criteria)	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Privacy Policies (10.1.0)	The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.	Monitoring and enforcement of privacy policies and procedures are informal and ad hoc. Guidance on conducting such reviews is not documented.	Monitoring and enforcement provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.	Monitoring and enforcement provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with monitoring and enforcement provisions in privacy policies is monitored and results are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to monitoring and enforcement. Issues of non-compliance are identified and remedial action taken to ensure compliance.
Communication to Individuals (10.1.1)	Individuals are informed about how to contact the entity with inquiries, complaints and disputes.	Individuals may be informed about how to contact the entity with inquiries, complaints and disputes; however, communications are inconsistent, sporadic and undocumented.	Procedures are in place to inform individuals about how to contact the entity with inquiries, complaints, and disputes but may not cover all aspects and are not fully documented.	Individuals are informed about how to contact the entity with inquiries, complaints and disputes and to whom the individual can direct complaints. Policies and procedures are documented and implemented.	Communications are monitored to ensure that individuals are adequately informed about how to contact the entity with inquiries, complaints and disputes.	Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required. Remedial action is taken when required.

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MONITORING and ENFORCEMENT (7 criteria) cont.	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Inquiry, Complaint and Dispute Process (10.2.1)	A process is in place to address inquiries, complaints and disputes.	An informal process exists to address inquiries, complaints and disputes; however, it is incomplete and inconsistently applied.	Processes to address inquiries, complaints and disputes exist, but are not fully documented and do not cover all aspects.	Documented policies and procedures covering all relevant aspects have been implemented to deal with inquiries, complaints and disputes.	Inquiries, complaints and disputes are recorded, responsibilities assigned and addressed through a managed process. Recourse and a formal escalation process are in place to review and approve any recourse offered to individuals.	Management monitors and analyzes the process to address inquiries, complaints and disputes and makes changes to the process, where appropriate.
Dispute Resolution and Recourse (10.2.2)	Each complaint is addressed, and the resolution is documented and communicated to the individual.	Complaints are handled informally and inconsistently. Adequate documentation is not available.	Processes are in place to address complaints, but they are not fully documented and may not cover all aspects.	Documented policies and procedures covering all relevant aspects have been implemented to handle privacy complaints. Resolution of the complaints is documented.	Privacy complaints are reviewed to ensure they are addressed within a specific time-frame in a satisfactory manner; satisfaction is monitored and managed. Unresolved complaints are escalated for review by management.	Privacy complaints are monitored and analyzed and the results used to redesign and improve the privacy complaint process.
Compliance Review (10.2.3)	Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreements and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	Review of compliance with privacy policies and procedures, laws, regulations and contracts is informal, inconsistently and incomplete.	Policies and procedures to monitor compliance with privacy policies and procedures, legislative and regulatory requirements and contracts are in place, but are not fully documented and may not cover all aspects.	Documented policies and procedures that cover all relevant aspects have been implemented that require management to review compliance with the entity's privacy policies and procedures, laws, regulations, and other requirements.	Management monitors activities to ensure the entity's privacy program remains in compliance with laws, regulations and other requirements.	Management analyzes and monitors results of compliance reviews of the entity's privacy program and proactively initiates remediation efforts to ensure ongoing and sustainable compliance.
Instances of Noncompliance (10.2.4)	Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.	Processes to handle instances of non-compliance exist, but are incomplete, informal and inconsistently applied.	Policies and procedures are in place to document non-compliance with privacy policies and procedures, but are not fully documented or do not cover all relevant aspects. Corrective and disciplinary measures may not always be documented.	Documented policies and procedures covering all relevant aspects have been implemented to handle instances of non-compliance with privacy policies and procedures. Corrective and disciplinary measures of non-compliance are fully documented.	Management monitors noncompliance with privacy policies and procedures and takes appropriate corrective and disciplinary action in a timely fashion.	Non-compliance results in disciplinary action and remedial training to correct individual behavior. In addition policies and procedures are improved to assist in full understanding and compliance.

Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MONITORING and ENFORCEMENT (7 criteria) cont.	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
Ongoing Monitoring (10.2.5)	Ongoing procedures are performed for monitoring the effectiveness of controls over personal information based on a risk assessment and for taking timely corrective actions where necessary.	Ongoing monitoring of privacy controls over personal information is informal, incomplete and inconsistently applied.	Monitoring of privacy controls is not fully documented and does not cover all aspects.	The entity has implemented documented policies and procedures covering all relevant aspects to monitor its privacy controls. Selection of controls to be monitored and frequency with which they are monitored are based on a risk assessment.	Monitoring of controls over personal information is performed in accordance with the entity's monitoring guidelines and results analyzed and provided to management.	Monitoring is performed and the analyzed results are used to improve the entity's privacy program. The entity monitors external sources to obtain information about their privacy "performance" and initiates changes as required.



**CONFIDENTIAL**

June 22, 2017

File: 7820-20-HSS-151-139

MS. DEBBIE DELANCEY
DEPUTY MINISTER
HEALTH AND SOCIAL SERVICES**Management Letter: Immunization Registry Processes**
Review Period: As of October 31, 2016

The Audit Committee approved the review and documentation of key processes in the Public Health Registries (PHR) unit in the Population Health Division, Department of Health and Social Services (Department). Through discussion with PHR management, the scope was narrowed down to focusing on the NWT Immunization Registry (Registry). The objectives were to collaborate with management and staff to document Registry processes, identify key controls used to manage risk, and support the capacity building of Registry staff in business process mapping.

From September 2016 to November 2016, the Internal Audit Bureau (IAB) interviewed PHR staff which included a field visit to Hay River in October 2016 to gather information from the PHR officer on the key processes to maintain the Registry. Five Registry process flowcharts as of October 31, 2016 were documented **(Appendix A and B refers)**.

To build the capacity of Registry staff, the IAB conducted a business process mapping demonstration during the field visit in Hay River. As a result, Registry staff independently prepared the fifth flow chart **(Appendix B refers)**.

While documenting the processes, the IAB noted inefficiencies and risk areas during the data entry of vaccine information and the subsequent validation phases. Other risks related to weakened information integrity, privacy risk, and the risk of file

and/or data corruption. These risks identified on the flowcharts in red, with additional details in the risk narrative (**Appendix A refers, page 6 of 6**) were presented to PHR management.

With PHR management's support, the IAB developed a risk assessment based on the control weaknesses outlined in the flowcharts (**Schedule 1 refers**). The inability to transfer relevant Electronic Medical Records (EMR) information to the Registry was a major source of risk. To mitigate this, the Chief Public Health Officer (CPHO) exercised his authority under the *Public Health Act* s.5 to allow the transfer of relevant immunization data from the EMR to the Registry.

Management updated the last column of Schedule 1, "Risk Mitigation Plan", with actions taken to mitigate the residual risk (**Schedule 1 refers**). The IAB or an independent contractor could be engaged to provide an independent, objective assessment to Senior Management on the steps taken to strengthen internal controls and mitigate the risks.

We would like to thank the Department staff for their assistance and cooperation during this project. Should you require additional information, please contact me at 767-9175 ext.15215.

Sincerely,



T. Bob Shahi
Director, Internal Audit Bureau

- c. Mr. Jamie Koe, Chair, Audit Committee
Dr. Andre Corriveau, Chief Public Health Officer, HSS
Ms. Laura Seddon, Director, Population Health, HSS
Ms. Jeannie Mathison, Director, Finance, HSS

SCHEDULE 1

Immunization Registries Risk Assessment as of October 31, 2016

Objective	Risk/Event	Trigger/Cause	Consequence/Impact	Inherent Risk			Risk Owner	Corporate Controls	Dept. Specific Controls	Residual Risk			Risk Mitigation Plan
				*L	*I	Risk without mgmt. controls				*L	*I	Risk based on existing mgmt. controls	
1. The legislative and regulatory framework for the immunization registry (IR) is followed.	The Public Health Registries (PHR) unit has no system in place to ensure that front-line staff comply with the required legislative and regulatory framework.	Access to relevant and timely data is restricted. Other than informal business processes (i.e. email reminders), the IR has no documented operating procedures on how to comply with applicable legislative and regulatory requirements.	IR data collection efforts were duplicated (for clinical and legislative reporting processes), resulting in an inefficient allocation of staff resources. IR data collected for the Chief Public Health Officer (CPHO) is inaccurate & incomplete. Data from front-line staff may not be submitted within the 4 week legislated timeframe. Non-compliance with Legislation and Regulations.	5	3	High	Pop. Health Division Director CPHO	Immunization Regulations s.3(4): unless otherwise stated, the information referred to in s.3.1 (a) to (l) must be provided within 4 weeks after the day the immunization is administered.	Informal business processes (i.e. email reminders)	5	3	High	Develop an operating policy that will give the PHR Unit a mechanism to obtain registry data from existing electronic information systems (eg., the electronic medical record or EMR) to manage the Immunization Registry as required by legislation and regulations. Obtain CPHO approval for the policy. Date: May 17, 2017 Completed by: PHR Manager, CPHO
2. Collection of accurate IR data.	The PHR unit was receiving inaccurate IR data from the NWT health centres and public health units.	Vaccine data collection at the NWT health centres is a manual process (hand written vaccine cards are data entered into Excel spreadsheets).	Inaccurate information used to compute coverage rates, indicators and other statistics. Decision making based on inaccurate data (i.e. Incorrect quantities requested on vaccine orders, improper coverage rates and inaccurate population health indicators and other statistics).	5	2	Medium	Pop. Health Division Director CPHO	Regulations s. 3(1): A health care professional who administers a notifiable immunization to a person shall ensure the CPHO is provided in an approved form, information respecting (a) to (l). Regulations s. 3(4): Unless otherwise stated, the information referred to in s.3.1 (a) to (l) must be provided within four weeks after the day the immunization is administered.	The PHR Officer conducts a comparison of health centre /public health unit data and electronic information using Excel validation tool. The community health centres/ public health units use an Excel spreadsheet template with predefined fields.	3	4	Medium	Access to EMR immunization records to improve data quality. Date: May 17, 2017 and ongoing Completed by: PHR Manager

*L= Probability that event will occur based on historical information

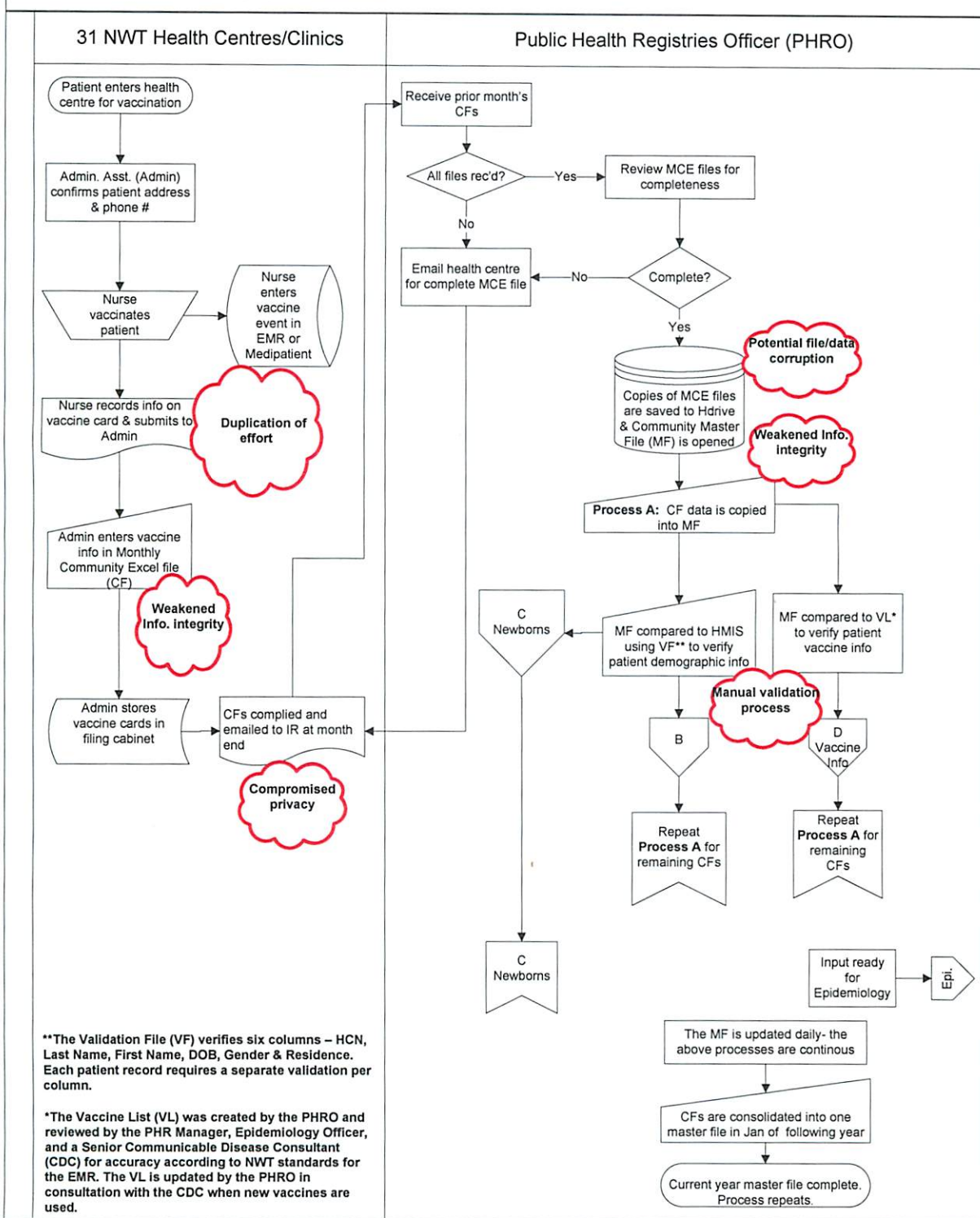
*I= Impact level based on the listed consequences

SCHEDULE 1

	Objective	Risk/Event	Trigger/Cause	Consequence/Impact	Inherent Risk			Risk Owner	Corporate Controls	Dept. Specific Controls	Residual Risk			Risk Mitigation Plan
					*L	*I	Risk without mgmt. controls				*L	*I	Risk based on existing mgmt. controls	
3.	Efficient IR Processes	The PHR unit's process for collecting immunization events (events) was redundant and inefficient	IR data collection efforts were duplicated by NWT health centres and public health units (for clinical and legislative reporting processes).	Health centre/public health nurse & admin compiling events to transfer to PHR Officer taking time away from their normal duties. PHRO spent 75% of time verifying accuracy of events & correcting errors from the 33 excel spreadsheet received each month.	5	3	High	Pop. Health Division Director CPHO	Regulations s. 3(1): A health care professional who administers a notifiable immunization to a person shall ensure the CPHO is provided in an approved form, information respecting (a) to (l).	The PHR officer conducts a comparison of health centre/public health units data and electronic information using Excel validation tool Excel spreadsheet template with predefined fields.	5	3	High	Access to electronic medical record immunization records to improve efficient collection of IR data Date: October 1, 2016 - May 17, 2017 Completed by: PHR Manager
4.	The privacy of patients that received vaccinations is maintained.	IR data may be emailed to the incorrect recipient without using Secure File Transfer (SFT) and password protection.	The IR processes for sending the monthly community Excel files using SFT and passwords are undocumented and not communicated to new staff due to staff turnover at the health centres and public health units.	Health information privacy breach; The patients may complain to the Privacy Commissioner or sue the GNWT; staff responsible for the breach may be disciplined.	5	4	Extreme	Pop. Health Division Director CPHO	Regulations s. 3(1): A health care professional who administers a notifiable immunization to a person shall ensure the CPHO is provided in an approved form, information respecting (a) to (l). Health Information Act s. 86 (2): Reasonable measures shall be taken to protect the security and confidentiality of personal health information. GNWT Oath of Office and Secrecy.	Use Secure File Transfer (SFT) and password protection when sending vaccination data to the PHR Officer.	3	4	Medium	Access to EMR immunization records to mitigate privacy risk. Encrypt IR data. Date: May 17, 2017 Completed by: PHR Manager

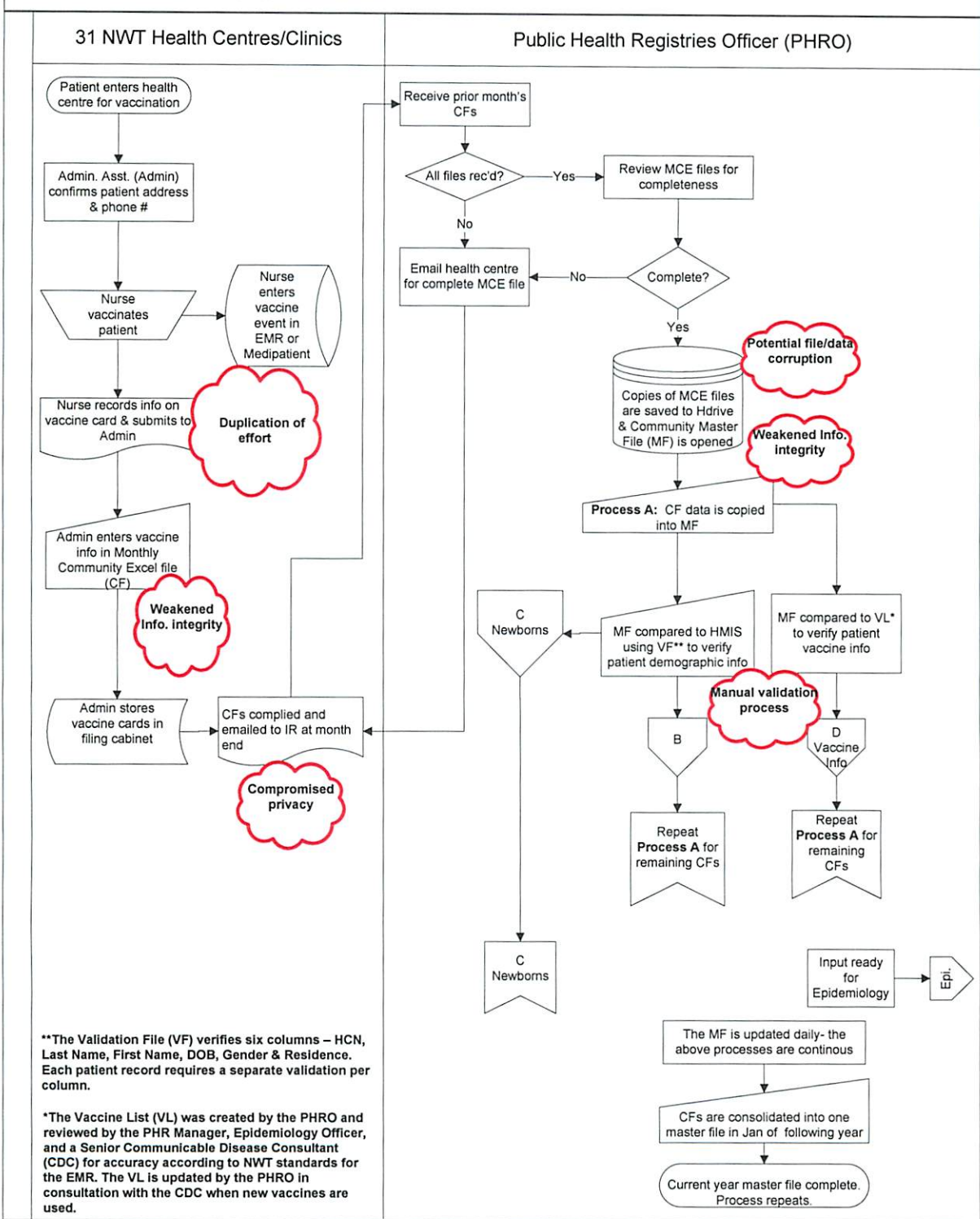
*L= Probability that event will occur based on historical information
 *I= Impact level based on the listed consequences

Immunization Registry (IR) Processes



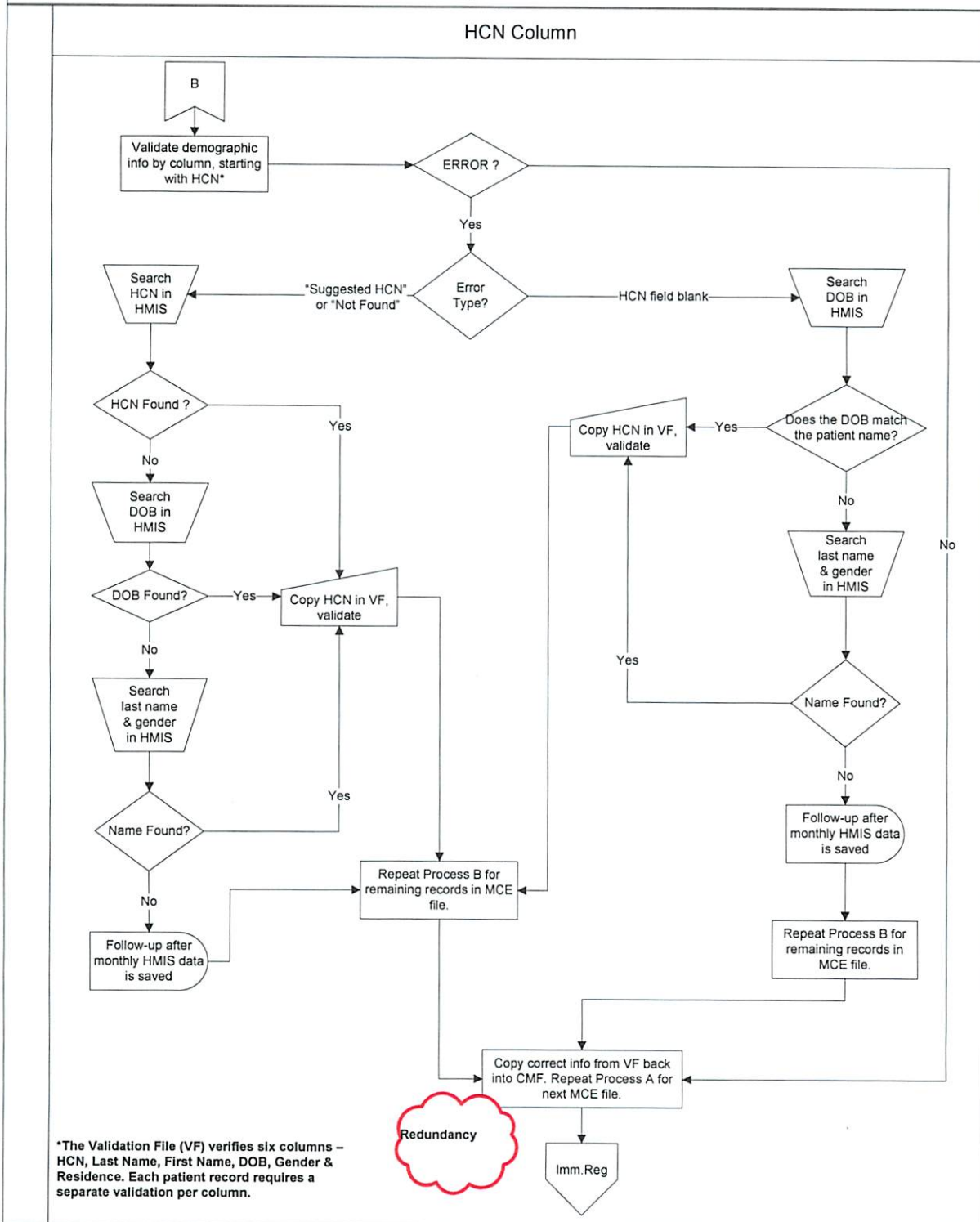
Appendix A

Immunization Registry (IR) Processes

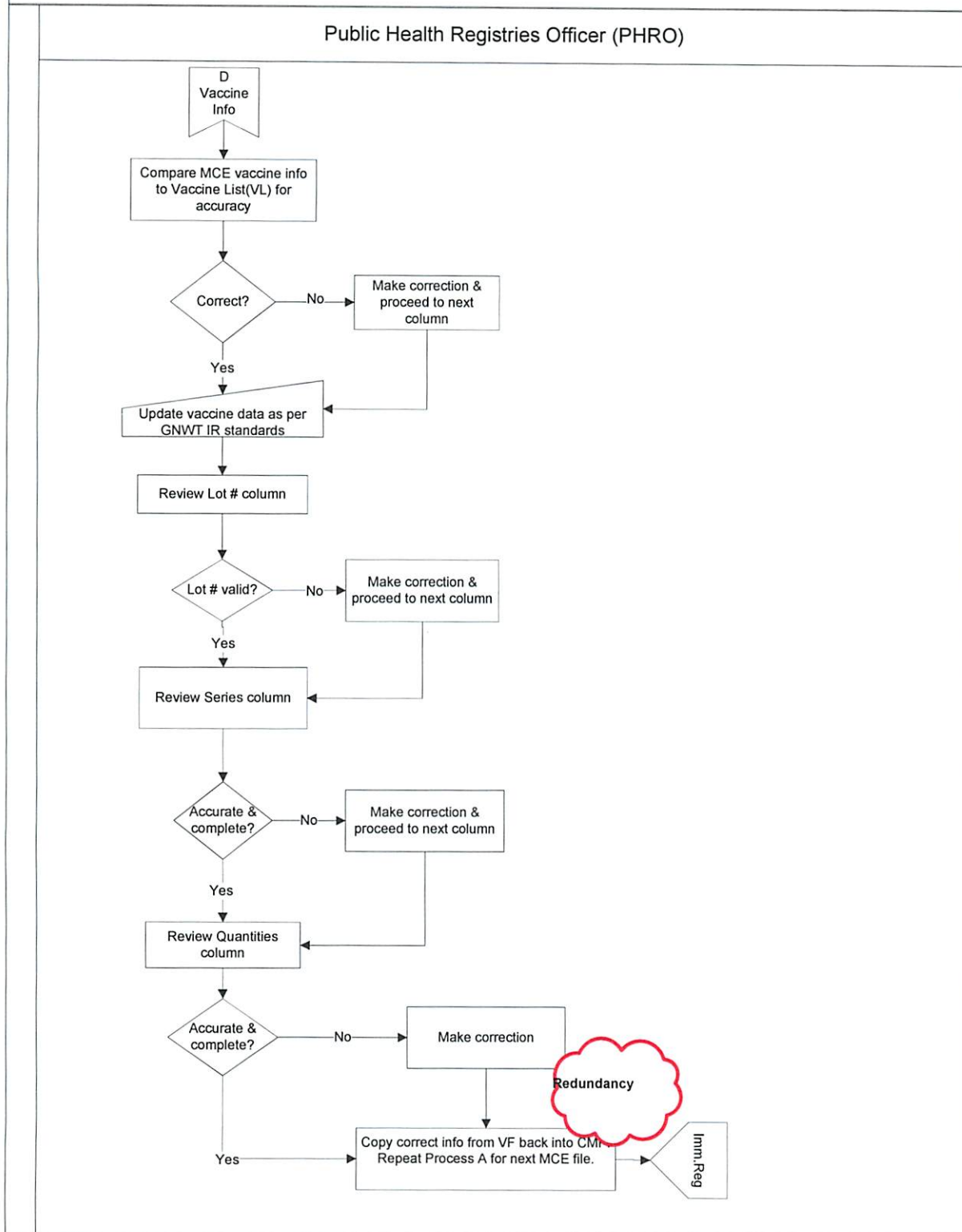


Appendix A

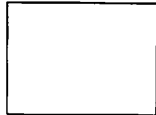
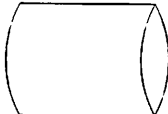
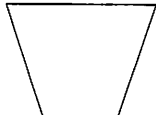

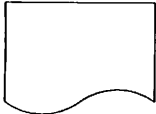
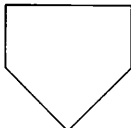
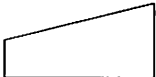
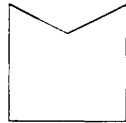
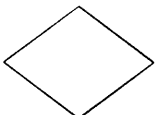
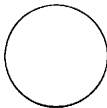
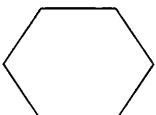
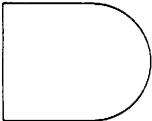


Process B: HMIS Validation Per Column Using Excel Validation File



Process D: Validation Of Vaccine Information



Appendix A

Legend			
	Process – instructions/actions to be performed		Direct Data – used to represent information systems
	Manual Operation		Stored data – represents storage point in process – associated with physical storage of documents
	Document – represents a document creation point in the process		Off-page reference - outgoing
	Manual input		Off-page reference - incoming
	Decision – shows decisions that must be made		On-page reference
	Preparation – handling step – multiple documents aggregated to make a package		
	Delay		
	Input Output symbol		
	Database – used to store electronic information		

Risk Narrative

The Internal Audit Bureau (IAB) visited the Hay River Health & Social Services Authority to observe the Immunization Registry (IR) data collection processes. The processes were documented on flowcharts starting from when a patient enters the vaccination facility, to the email transmission of vaccine information to the IR, and its retrieval from the Epidemiology and Surveillance Unit (ESU) for analysis and reporting.

According to section 2 of the Immunization Regulations (Regulations), if a health care professional is notified of an adverse reaction to a vaccine, the health care professional must provide the CPHO with a copy of the *Report of Adverse Events Following Immunization (AEFI)* within 24 hours of the notification. The IAB noted that this information is recorded in the Electronic Medical Records (EMR); however, it is unclear if the CPHO was receiving a copy of the AEFI within 24 hours of the notification.

According to section 3(1) of the Regulations, a health care professional administering a notifiable immunization shall ensure the Chief Public Health Officer (CPHO) is provided with the patient's detailed demographic and vaccination information in an approved form. Section 4 of the Regulations state that the information must be provided within four weeks after the day the immunization is administered, unless the CPHO requests an earlier date. Based on the IAB's observations, it was unclear if the CPHO was provided with the information within the four week deadline as per Section 4 of the Regulations.

The IAB noted a duplication of work in the data entry of the information requirements. The EMR contains parts (a) to (e) from the Regulations, which is preexisting data from the patient's medical chart. When a patient is vaccinated, the nurse data enters parts (f) to (l) in the EMR using predefined fields, this same information excluding part (l), is handwritten by the nurse on vaccine cards. The vaccine cards are then manually entered into a monthly Excel spreadsheet by administrative personnel, who email the file to the IR at month end.

The Public Health Registries Officer (PHRO) at the IR receives the Excel files from the NWT communities on a monthly basis, and validates the data for accuracy and completeness. The validation process compares the demographic data to information retrieved from HMIS. This process takes 75% of the PHRO's time, with vaccination volumes averaging 1800 per month. The vaccine information is compared to a vaccine list developed by IR and ESU staff. The vaccine comparison ensures that the vaccination data is recorded using the GNWT standard formatting. The data is stored on the IR Hdrive and accessed by the ESU when needed. The ESU conducts a separate review of the data to ensure correct demographic formatting.

Section 4(1) of the Regulations states that where a person refuses to be immunized, the health care professional who would have administered the immunization shall ensure the CPHO is provided in an approved form, information respecting the refusal. The IAB noted that this information is recorded in the EMR; however, it is unclear if the CPHO was receiving a copy of the refusals in an approved form.

HSS Public Health Registries Processes
Health & Social Services
FILE No: 7820-21-HSS-151-139
September 1, 2016 to October 31, 2016

Appendix B

Process C: Newborn Validations

