



**CONFIDENTIAL**

MAY 04 2018

File: 7820-20-GNWT-151-131

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**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 August 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. Mandi Bolstad, Director, Corporate Services, Justice



# JUSTICE

## Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



Government of Northwest Territories  
Gouvernement des Territoires du Nord-Ouest

## **JUSTICE**

### **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 4, 2018

File: 7820-20-GNWT-151-131

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**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 Justice was part of the overall audit project. This report identifies issues specific to your department.

In assessing the privacy of information for 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.*

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

The contractor assessed the compliance to the *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 the *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 at the “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 documented 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**)

There were only two recommendations made by the contractor:

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

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

**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.

		Internal Control Capacity Level				
		Ad-hoc	Repeatable	Defined	Managed	Optimized
<b>Privacy Risk Level</b>	Very High		<b>Justice</b>			
	High					
	Medium					
	Low					
	Very Low					
		Not Compliant	Partially Compliant	Compliant	Fully Compliant	Perfectly Compliant
		<b>Compliance Classification</b>				

Capacity required for addressing assessed risk



Resources used to build capacity for compliance purpose but unnecessary to address privacy risk

Risk Level and Internal Control Capacity Level are matched.

## DEPARTMENT OF JUSTICE

### 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 Justice (“Justice”) meets its responsibilities through programs it offers through its divisions of:

- Community Justice & Policing;
- Corporate Services;
- Corrections;
- Court Services;
  - Court Registries,
  - Court Reporters Office,
  - Sheriff’s office.
- Directorate;
- Legal;
- Legal Registries; and
- Policy and Planning.

Justice collects personal information through the divisions listed above as well as its boards and agencies:

- Coroner Service;
- Judicial Remuneration Commission;
- Legal Aid Commission;
- Maintenance Enforcement Program;
- Northwest Territories Review Board;
- Office of the Regulator of Oil and Gas Operations;
- Public Trustee Office;
- Rental Office; and



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

- Victims Assistance Committee.

Personal information collected as part of Coroner Services is governed by the Coroner's Act that includes notwithstanding clauses that result in this Act superseding ATIPP and as such personal information is collected under the Coroner's Act rather than ATIPP. Given that the department works to meet this legislation, rather than specifically ATIPP, the personal information managed under this Act has been excluded from the scope of this report.

Personal information collected as part of Corrections is stored on the APPGEN system, COMS database, FSCC Phone System, Genesis, Inmate Phone System, Lenel – NSCF, March Systems – NSCC, MHS, NSCC Phone System, Pelco – NSCC, SMCC Phone System and SMCC Security System. Personal information collected is also stored on Childview database, Appointments and Revocations Database, CSMNET, MEP Website, CanTax and Computrust.

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

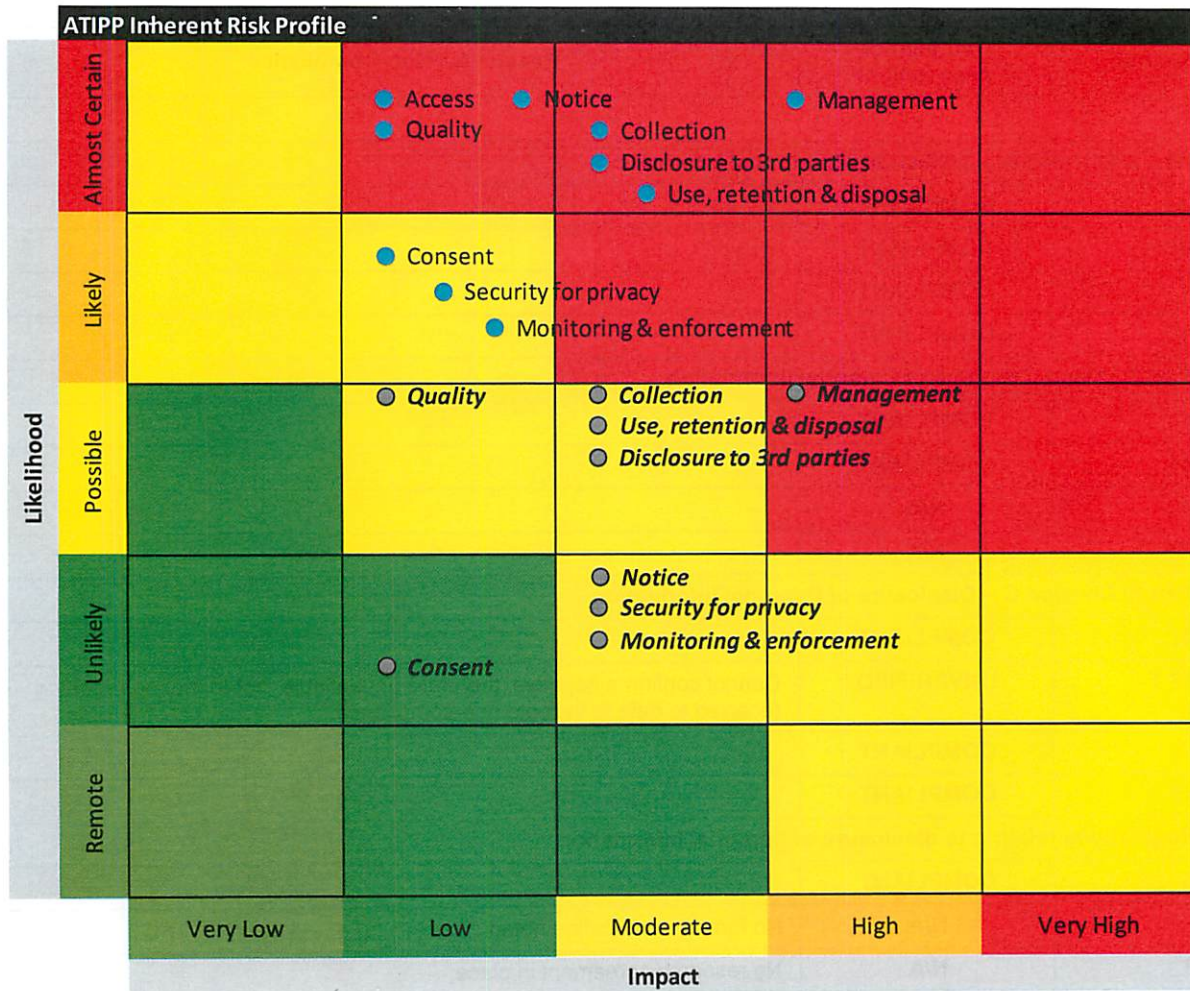
### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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.

**DEPARTMENT OF JUSTICE**

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

**RISK HEATMAP**



**Compliance with ATIPP Part 2 Protection of Privacy**

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

## DEPARTMENT OF JUSTICE

### 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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	N/A	
46	N/A	
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	COMPLIANT	
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	COMPLIANT	
<b>Regulations relating to disclosure of personal information</b>		
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).

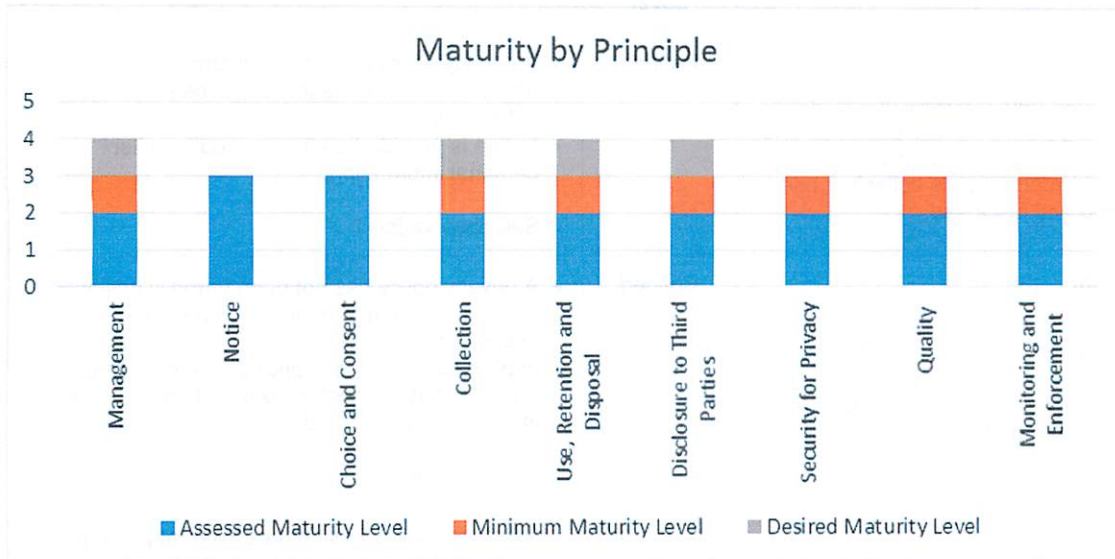
**Desired Maturity Level** – This level would be achieved via long term goals (>24 months) and should be part of long term planning if applicable to your department.

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

**DEPARTMENT OF JUSTICE**

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

adequate protection of data. Justice falls into this category, and is therefore expected to plan for the desired maturity level in the future.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP coordinator has been assigned and has taken the training offered by the Privacy Office and Manager of the GNWT Access and Privacy Office.</li> <li>The ATIPP coordinator has delegated authority to the department's senior information privacy analyst to assist with ATIPP requirements.</li> <li>ATIPP delegates review and approve procedures and new collection forms for ATIPP compliance however, reviews of pre-existing forms is not done.</li> <li>Privacy Impact Assessments have started to be used for new programs but have not been done for existing programs.</li> </ul> <p>See observations 1-2.</p>

## DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Notice</b></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"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is provided on forms used to collect personal information.</li> </ul> <p>See observation 1.</p>
<p><b>Consent</b></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>	Defined	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent and explicit consent is obtained on information collection forms when sensitive information is collected.</li> </ul> <p>See observation 1.</p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>The type of personal information collected and the method of collection is known to the individual and the department discloses the collection of information through the use of cookies.</li> <li>Methods and forms of collecting information are provided to the ATIPP coordinator for review before implementation to ensure collection is fair and by lawful means and is limited to that necessary for the purposes identified in the notice.</li> </ul> <p>See observations 1.</p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A formal procedure/process does not exist to ensure information collected is only used for the purpose for which it was collected; review by ATIPP coordinator is done on method of collection to ensure only information needed is collected.</li> <li>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.</li> </ul> <p>See observation 1.</p>

# DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Disclosure to third parties</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Information sharing agreements exist with other departments to provide instructions or requirements 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.</li> </ul> <p>See observation 1.</p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of Digital Integrated Information Management System (DIMs) and database restrictions put in place. Physical access to personal information is restricted through various safeguards.</li> <li>• Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>• Tests of safeguards in place are not performed.</li> </ul> <p>See observation 1.</p>
<p><b>Quality</b></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"> <li>• 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.</li> <li>• Methods of collecting information are provided to the ATIPP coordinator for review before implementation to ensure information collected is relevant for its use.</li> </ul> <p>See observation 1.</p>

## DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>Inquiry, complaint and dispute procedures exist but are not formally documented.</li> <li>Monitoring and enforcement are not being done at present.</li> </ul> <p>See observation 1.</p>

## Observations and Recommendations

### Observation 1

#### Privacy policy has not been designed and documented

- The ATIPP coordinator has limited time and resources to dedicate to ATIPP policies and procedures, specifically in regards to part 2 of the legislation.
- Procedures exist within divisional documents such as the Corrections Service Directives which address relevant privacy principles.

#### 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 who is manager of the office of the GNWT 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:
The Department of Justice, GNWT Access and Privacy Office has drafted a GNWT Protection of Privacy Policy which has been shared with all departments for review and discussion. It is anticipated that the Policy will be finalized by June 30, 2018.	June 2018

## DEPARTMENT OF JUSTICE

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

Justice departmental processes and procedures will be set up throughout the Department in order to meet the overarching policy and guidelines.	March 2019
The draft Protection of Privacy Policy is part of an overarching GNWT Privacy Framework that is being developed to support departments in ensuring that the privacy provisions of the ATIPP Act are administered in a consistent and fair manner. The framework will include Privacy Management Program guidelines which are intended to address the overall privacy risks, etc. These guidelines are drafted and are being reviewed by departments.	June 2018

#### 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.
- Third parties involved are not identified and documented.

##### Risk Profile:

Risk Impact	Without an inventory of personal information, it is not possible for the department to ensure that all areas containing personal information are adequately protected under ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP coordinator who is manager of the office of the GNWT Privacy Office

##### Recommendations:

We recommend that:

- An inventory of the types of personal information and the related processes, 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:
The Department of Justice will compile a listing of personal information collected by each division.	June 2018
It is unclear how third parties are defined in relation to this Audit but once clarified, the Department will include a listing of third parties in relation to the personal information inventory.	June 2018

Responses were provided by Denise Anderson with copies to Mandi Bolstad and Richard Robertson.



AICPA/CICA  
Privacy Maturity Model

March 2011



## Appendix A

### 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](http://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

# Appendix A

## AICPA/CICA Privacy Maturity Model

### 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](http://www.aicpa.org/privacy) and [www.cica.ca/privacy](http://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 Model<sup>1</sup> 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.

<sup>1</sup> 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

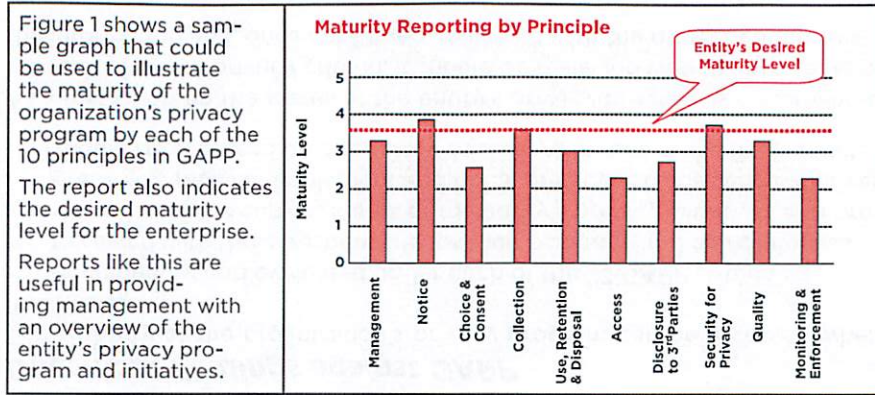


Figure 2 – Maturity Report by Criteria within a Specific GAPP Principle

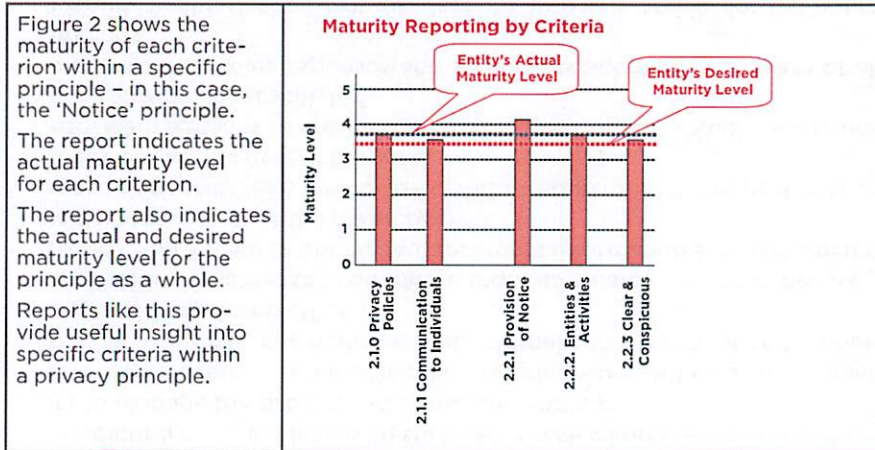
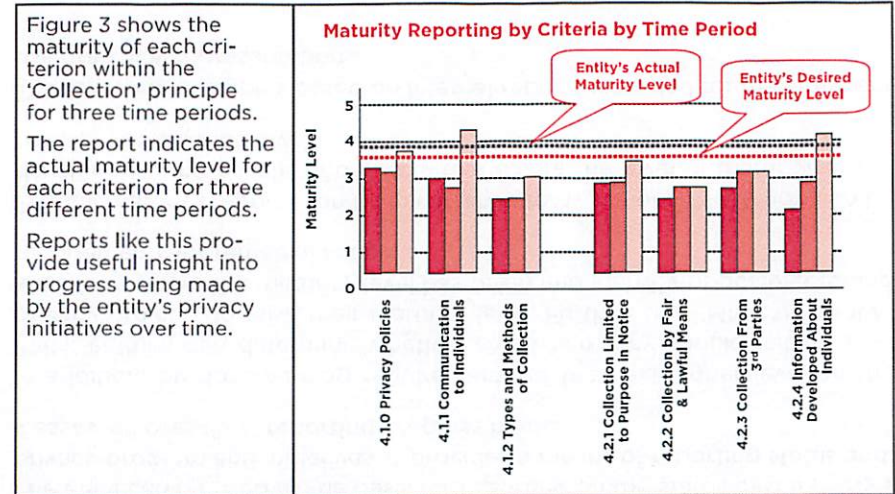


Figure 3 – Maturity Report by Criteria within a GAPP Principle Over Time



## 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 MODEL<sup>1</sup>

## Based on Generally Accepted Privacy Principles (GAPP)<sup>2</sup>

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria)</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Privacy Policies (1.1.0)</b>	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.
<b>Communication to Internal Personnel (1.1.1)</b>	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.

<sup>1</sup> 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.

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

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Responsibility and Accountability for Policies (1.1.2)</b>	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.
<b>Review and Approval (1.2.1)</b>	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.
<b>Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)</b>	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.

# Appendix A

## AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Personal Information Identification and Classification (1.2.3)</b>	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.
<b>Risk Assessment (1.2.4)</b>	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.
<b>Consistency of Commitments with Privacy Policies and Procedures (1.2.5)</b>	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.

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"> <li>• Infrastructure</li> <li>• Systems</li> <li>• Applications</li> <li>• Web sites</li> <li>• Procedures</li> <li>• Products and services</li> <li>• Data bases and information repositories</li> <li>• Mobile computing and other similar electronic devices</li> </ul> <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
<b>MANAGEMENT</b> (14 criteria) cont.	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Privacy Incident and Breach Management (1.2.7)</b>	<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"> <li>• Procedures for the identification, management and resolution of privacy incidents and breaches</li> <li>• Defined responsibilities</li> <li>• A process to identify incident severity and determine required actions and escalation procedures</li> <li>• A process for complying with breach laws and regulations, including stakeholder breach notification, if required</li> <li>• An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate</li> <li>• 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"> <li>— Incident patterns and root cause</li> <li>— Changes in the internal control environment or external requirements (regulation or legislation)</li> </ul> </li> <li>• Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed</li> </ul>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Supporting Resources (1.2.8)</b>	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.
<b>Qualifications of Internal Personnel (1.2.9)</b>	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.
<b>Privacy Awareness and Training (1.2.10)</b>	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.



## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Changes in Regulatory and Business Requirements (1.2.11)</b>	<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"> <li>– Legal and regulatory</li> <li>– Contracts, including service-level agreements</li> <li>– Industry requirements</li> <li>– Business operations and processes</li> <li>– People, roles, and responsibilities</li> <li>– Technology</li> </ul> <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.
<b>NOTICE (5 criteria)</b>	<b>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</b>					
<b>Privacy Policies (2.1.0)</b>	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.
<b>Communication to Individuals (2.1.1)</b>	<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
<b>NOTICE (5 criteria) cont.</b>	<b>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</b>					
<b>Provision of Notice (2.2.1)</b>	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).
<b>Entities and Activities Covered (2.2.2)</b>	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.
<b>Clear and Conspicuous (2.2.3)</b>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria)</b>	<b>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.</b>					
<b>Privacy Policies (3.1.0)</b>	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.
<b>Communication to Individuals (3.1.1)</b>	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.
<b>Consequences of Denying or Withdrawing Consent (3.1.2)</b>	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.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria) cont.</b>	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.					
<b>Implicit or Explicit Consent (3.2.1)</b>	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.
<b>Consent for New Purposes and Uses (3.2.2)</b>	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.
<b>Explicit Consent for Sensitive Information (3.2.3)</b>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria) cont.</b>	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.					
<b>Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices (3.2.4)</b>	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.
<b>COLLECTION (7 criteria)</b>	The entity collects personal information only for the purposes identified in the notice.					
<b>Privacy Policies (4.1.0)</b>	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.
<b>Communication to Individuals (4.1.1)</b>	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
<b>COLLECTION (7 criteria) cont.</b>		<b>The entity collects personal information only for the purposes identified in the notice.</b>				
<b>Types of Personal Information Collected and Methods of Collection (4.1.2)</b>	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.
<b>Collection Limited to Identified Purpose (4.2.1)</b>	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"> <li>• be fully documented;</li> <li>• distinguish the personal information essential for the purposes identified in the notice;</li> <li>• differentiate personal information from optional information.</li> </ul>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>COLLECTION (7 criteria) cont.</b>	<b>The entity collects personal information only for the purposes identified in the notice.</b>					
<b>Collection by Fair and Lawful Means (4.2.2)</b>	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.
<b>Collection from Third Parties (4.2.3)</b>	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.
<b>Information Developed About Individuals (4.2.4)</b>	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
<b>USE, RETENTION AND DISPOSAL (5 criteria)</b>	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.					
<b>Privacy Policies (5.1.0)</b>	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.
<b>Communication to Individuals (5.1.1)</b>	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 to individuals 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.
<b>Use of Personal Information (5.2.1)</b>	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.



## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>USE, RETENTION AND DISPOSAL (5 criteria) cont.</b>	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.					
<b>Retention of Personal Information (5.2.2)</b>	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.
<b>Disposal, Destruction and Redaction of Personal Information (5.2.3)</b>	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.
<b>ACCESS (8 criteria)</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Privacy Policies (6.1.0)</b>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Communication to Individuals (6.1.1)</b>	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.
<b>Access by Individuals to their Personal Information (6.2.1)</b>	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 be 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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Confirmation of an Individual's Identity (6.2.2)</b>	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.
<b>Understandable Personal Information, Time Frame, and Cost (6.2.3)</b>	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
<b>ACCESS (8 criteria) cont.</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Denial of Access (6.2.4)</b>	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.
<b>Updating or Correcting Personal Information (6.2.5)</b>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Statement of Disagreement (6.2.6)</b>	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.
<b>DISCLOSURE TO THIRD PARTIES (7 criteria)</b>	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.					
<b>Privacy Policies (7.1.0)</b>	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.
<b>Communication to Individuals (7.1.1)</b>	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.

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>	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.					
<b>Communication to Third Parties (7.1.2)</b>	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.
<b>Disclosure of Personal Information (7.2.1)</b>	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.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>	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.					
<b>Protection of Personal Information (7.2.2)</b>	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.
<b>New Purposes and Uses (7.2.3)</b>	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
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>	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.					
<b>Misuse of Personal Information by a Third Party (7.2.4)</b>	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.
<b>SECURITY FOR PRIVACY (9 criteria)</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Privacy Policies (8.1.0)</b>	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.
<b>Communication to Individuals (8.1.1)</b>	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.



# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Information Security Program (8.2.1)</b>	<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 areas<sup>3</sup> insofar as they relate to the security of personal information:</p> <ul style="list-style-type: none"> <li>a. Risk assessment and treatment [1.2.4]</li> <li>b. Security policy [8.1.0]</li> <li>c. Organization of information security [sections 1, 7, and 10]</li> <li>d. Asset management [section 1]</li> <li>e. Human resources security [section 1]</li> <li>f. Physical and environmental security [8.2.3 and 8.2.4]</li> <li>g. Communications and operations management [sections 1, 7, and 10]</li> <li>h. Access control [sections 1, 8.2, and 10]</li> <li>i. Information systems acquisition, development, and maintenance [1.2.6]</li> <li>j. Information security incident management [1.2.7]</li> <li>k. Business continuity management [section 8.2]</li> <li>l. Compliance [sections 1 and 10]</li> </ul>	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.

<sup>3</sup> 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](http://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
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Logical Access Controls (8.2.2)</b>	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ol style="list-style-type: none"> <li>a. Authorizing and registering internal personnel and individuals</li> <li>b. Identifying and authenticating internal personnel and individuals</li> <li>c. Making changes and updating access profiles</li> <li>d. Granting privileges and permissions for access to IT infrastructure components and personal information</li> <li>e. Preventing individuals from accessing anything other than their own personal or sensitive information</li> <li>f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities</li> <li>g. Distributing output only to authorized internal personnel</li> <li>h. Restricting logical access to offline storage, backup data, systems and media</li> <li>i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</li> <li>j. Preventing the introduction of viruses, malicious code, and unauthorized software</li> </ol>	<p>Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete.</p>	<p>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>	<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>

# Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Physical Access Controls (8.2.3)</b>	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.
<b>Environmental Safeguards (8.2.4)</b>	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.
<b>Transmitted Personal Information (8.2.5)</b>	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.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Personal Information on Portable Media (8.2.6)</b>	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.
<b>Testing Security Safeguards (8.2.7)</b>	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.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>QUALITY (4 criteria)</b>	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
<b>Privacy Policies (9.1.0)</b>	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.
<b>Communication to Individuals (9.1.1)</b>	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.
<b>Accuracy and Completeness of Personal Information (9.2.1)</b>	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
<b>QUALITY (4 criteria) cont.</b>	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
<b>Relevance of Personal Information (9.2.2)</b>	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.
<b>MONITORING and ENFORCEMENT (7 criteria)</b>	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
<b>Privacy Policies (10.1.0)</b>	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.
<b>Communication to Individuals (10.1.1)</b>	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.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MONITORING and ENFORCEMENT (7 criteria) cont.</b>	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
<b>Inquiry, Complaint and Dispute Process (10.2.1)</b>	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.
<b>Dispute Resolution and Recourse (10.2.2)</b>	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.
<b>Compliance Review (10.2.3)</b>	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.
<b>Instances of Noncompliance (10.2.4)</b>	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
<b>MONITORING and ENFORCEMENT (7 criteria) cont.</b>	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
<b>Ongoing Monitoring (10.2.5)</b>	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.



## Appendix A

AICPA/CICA Privacy Maturity Model

### **NOTES**

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

Appendix A





## Justice

### Yellowknife Court Trust Account And Sheriff Trust Account

Internal Audit Bureau – Audit Report  
January 2017



**CONFIDENTIAL**

January 26, 2017

File: 7820-20-JUS-151-116 and;  
7820-20-JUS-151-117

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**Audit Report: Yellowknife Court Trust Account**  
**Audit Period: March 1, 2015 to March 31, 2016**

**Audit Report: Sheriff Trust Account**  
**Audit Period: October 1, 2013 to January 31, 2016**

---

**A. SCOPE AND OBJECTIVES**

The Audit Committee approved the Department of Justice (Department) management requested audits of the Yellowknife Court Registry and Sheriff Trust accounts (Trust Accounts). The audit objectives were to assess the internal control capacity in managing the Trust Accounts, to determine if the:

- Department legislation, policies and procedures were adequate to process trust account transactions as required by the Financial Administration Manual (FAM)
- information used to monitor the trust accounts was relevant, reliable, accurate, complete, and timely
- Financial Administration Act (FAA), FAM, management policies and procedures were followed
- assets were protected
- processes were efficient and effective.

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's Court Services Division (Court Services) delivered services supporting the activities of the Northwest Territories (NWT) Courts. NWT Courts included the:

- Court of Appeal for the NWT
- Supreme Court of the NWT
- Territorial Court of the NWT
- Youth Justice Court of the NWT
- Justice of the Peace Court of the NWT

NWT Courts operated independently of the Executive branch of the Government of the NWT (GNWT). Court Services supported the activities of the NWT Courts by managing the Court Library, Court Registries, Sheriff's Office and Court Reporter's Office.

NWT Courts were responsible for administering money paid into Court on behalf of clients. The Department held the money paid into Court in the Trust Accounts authorized by the GNWT Comptroller General.

### **YK Court Trust Account**

Court Registries were the public offices of the NWT Courts and were located in Yellowknife, Hay River, and Inuvik. Court Registries managed court files and was responsible for court administrative activities such as accepting fine and restitution payments, filing documents, and providing certified copies of court orders. Each Court Registry had its own trust account including the Yellowknife Court Registry (YK Court Registry). We audited the YK Court Registry Trust Account (YK Court trust account).

Prior to 2001, YK Court Registry had trust accounts for the Supreme Court and Territorial Court. In September 2001, Management merged the accounts into the YK Court trust account. The YK Court trust account had approximately 3,500 transactions per year and the March 31, 2016 year to date balance was over \$800,000.

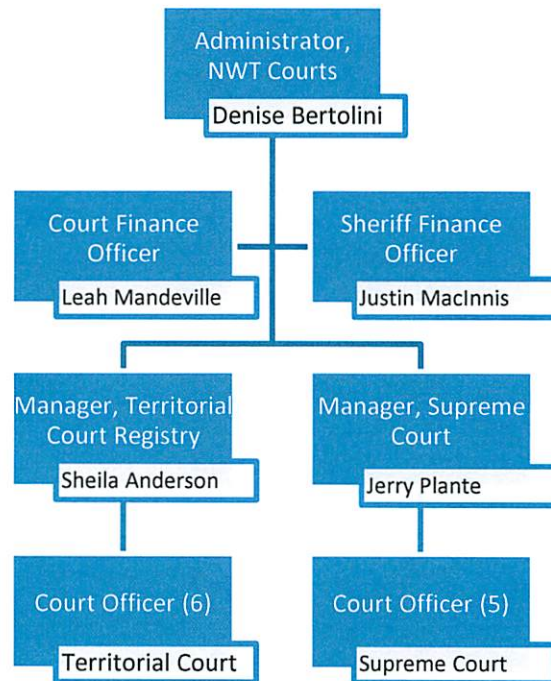
### **Sheriff Trust Account**

The Sheriff's Office was authorized by writs or court orders to execute seizures, remove goods, lands, and tenant evictions. Writs were court orders enabling a creditor to collect on a debt by garnishment or seizure of the debtor's property. We conducted an audit on the Sheriff Trust account. The Sheriff Trust account

had approximately 800 writ transactions per year and the March 31, 2016 year to date balance was \$350,000.

### Trust Accounts Roles and Responsibilities

In 2015-2016, Court Services had an annual operating budget of over \$14 million. Out of the 62 full time positions in Court Services, 16 had roles in processing Trust Accounts transactions.



The Administrator, NWT Courts (Administrator) was responsible for the NWT Courts human resources, financial, administrative and system needs, while balancing the requirements of the judiciary and the Department. The Administrator:

- held seven statutory appointments and reported to the Judges of the Supreme and Territorial Courts on the judiciary responsibilities
- was accountable for the Trust Accounts and reported to the Director of Court Services on the Department responsibilities.

The Court Finance Officer and the Sheriff Finance Officer reported to the Administrator and were responsible for the regular maintenance and safekeeping of the Trust Accounts (**Appendix A refers**).

Court Officers reported to their Manager, Territorial Court Registry and Supreme Court and were responsible for processing the incoming payments in FACTS (information system to track court cases) and forwarded them to the Court and

Sheriff Finance Officers to prepare the deposits, disbursements and bank reconciliations. The Administrator approved the bank reconciliations and forwarded them to the Department's Finance Division for recording the monthly balance into the GNWT financial system.

## C. OVERVIEW

The independence of the judiciary in the Westminster model has been well accepted in the commonwealth nations. The responsibility for administration of court operations resided with the Executive branch of the GNWT, specifically, with the Department's Administrator. As such, the Administrator was required to follow the GNWT financial administration, FAA and FAM governance framework.

Processing the NWT judiciary court orders and related trust account transactions had a high level of inherent risk. To address this and other operational challenges, Court Registries required an internal control capacity where controls were documented to ensure consistency and control gaps were identified and remediated in a timely manner. Management implemented internal controls that reduced the risk to a moderate level. With additional steps the risks may be further reduced.

At the time of the audit, we noted the GNWT had a documented governance framework for handling public money and the Court Registries had procedures for processing court orders. However, there was little to no direction on handling public money held in trust. The lack of clear direction contributed to the non-compliance with the *Creditors Relief Act*, FAM and inefficient client services observed during the audit. Streamlining the internal process with clear written direction on key controls to manage the risk, would allow the Court Registries to meet the needs of the client, the judiciary, and GNWT.

Issues identified with approval authorities, receipt and deposit of public money and accountable forms control were addressed by Management during the audit.



## D. OBSERVATIONS AND RECOMMENDATIONS

### 1. Refunds

#### Observation:

Since 2003, over \$11,000 in accumulated residual Sheriff's fee deposits were not refunded to clients.

*Judicature Act, Rules of the Supreme Court of the NWT* s. 213 (1) Closing of account allowed for the NWT Courts to close the account and transfer a credit balance to the Consolidated Revenue Fund when:

- the credit balance was \$100 or less and 2 years elapsed since the money was paid out of court
- 10 years elapsed since the money was paid out of court.

The *Creditors Relief Act* required creditors to pay a deposit to the Sheriff Office to receive civil enforcement services. Court Registries explained that the difference between the deposit and the actual service cost was refunded to the creditor or collected from the creditor. The February 2016 Excel spreadsheet provided by the Sheriff Finance Officer showed an "Aged Overpayments" tab that had 178 outstanding cases with a balance of \$11,108 of un-refunded client money. We noted:

- amounts owing to clients ranging from \$0.25 to \$1,318
- dates of last transaction from, "pre-2003 too old to tell" to "December 2014"
- 130 cases with no date of last transaction totalling \$8,900
- Sheriff Finance Officer made an effort to contact clients in 48 cases
- Out of the 48 cases, 42 were over two years old and had \$100.00 or less amounts owing totalling \$1,190.

The 42 cases that the Sheriff Finance Officer followed up on met the requirements to have their accounts closed and their balances transferred. The 130 cases with the amount owing of \$8,900 required effort to clear the outstanding balance.

There was no evidence of documented accountability to close the accounts within the defined timelines or to refund the client money. The challenge of contacting the clients increases as the refund due ages. While some of the clients may still reside in the NWT or other jurisdictions, there was likelihood that some client account balances may closed without refunding the client.

**Risk Profile:**

<b>Risk Impact Level:</b>	Moderate: Requires specific allocation of management responsibility to refund client money.
<b>Risk Responsibility:</b>	Deputy Minister, Justice
<b>Risk Mitigation Support:</b>	<ul style="list-style-type: none"> <li>• Director, Court Services, Justice</li> <li>• Director, Finance &amp; Administration, Justice</li> <li>• Yellowknife Court Registries Administrator, Justice</li> </ul>

**Recommendation:**

We recommend that Court Services:

- a) Comply with s. 213(1) of the *Judicature Act – Rules of the Supreme Court*
- b) escalate any accounts not closed within the timeline and amounts not refunded to Senior Management for additional guidance.

**Management Response:**

<b>Action Plan</b>	<b>Completion Date:</b>
<p>a) <i>Management will review procedures on deposits received for the Sheriff's Trust Account and document procedures for complying with s.213 (1) of the Judicature Act.</i></p> <p>b) <i>Management agrees with this recommendation, escalation will be part of the documented procedures described above.</i></p>	<p>a) March 2017 b) March 2017</p>

## 2. Record Conversion

### Observation:

Court Registries held over \$85,000 of undisbursed client money due to the incomplete transfer of records during the conversion to FACTS in 2009.

In accordance with FAM 1301 (now 205) Internal Control, GNWT Departments must have adequate internal controls, including independently maintained control accounts. Adequate internal controls would require that all information transferred was accurate and complete upon converting to a new financial information system.

During our review of the bank reconciliations of the Trust Accounts, we observed that \$87,650 was outstanding:

- The YK Court trust account had an outstanding amount of \$85,400 recorded as "*Simply Accounting Balance – GL*"
- The Sheriff Trust account had an outstanding amount of \$2,250 recorded as "*G/L Balance – Simply Accounting*".

Management confirmed that the amounts noted above represented monies owing to clients carried forward when Court Registries converted their Simply Accounting financial system to the FACTS information system in 2009.

There was no evidence of documented accountability to clear the outstanding balances within defined timelines. The challenge of contacting the clients increases as time passes. While some of the client may still reside in the NWT or other jurisdictions, there was likelihood that some client account balances may not be cleared.

**Risk Profile:**

<b>Risk Impact Level:</b>	Moderate: Requires specific allocation of management responsibility to clear the outstanding balance.
<b>Risk Responsibility:</b>	Deputy Minister, Justice
<b>Risk Mitigation Support:</b>	<ul style="list-style-type: none"><li>• Director, Court Services, Justice</li><li>• Director, Finance &amp; Administration, Justice</li><li>• Administrator, NWT Courts, Justice</li></ul>

**Recommendation:**

We recommend that Court Services:

- a) clear the outstanding “undisbursed client money” balances
- b) escalate any amount not cleared by January 31, 2017 to Senior Management for additional guidance.

**Management Response:**

<b>Action Plan</b>	<b>Completion Date:</b>
<i>a) Management agrees with this recommendation,</i> <i>b) Management agrees with this recommendation.</i>	a) January 31, 2017 b) January 31, 2017

### 3. Incoming Mail Deposits

#### Observation

Over \$340,000 of mailed-in cheques were not kept safe and not deposited into the Trust Accounts for up to three weeks.

FAM 2904 (now 415) Receipt and Deposit of Public Money, requires:

- incoming mail should be opened in the presence of at least two public officers where possible
- the Daily Register of Incoming Revenue (DRIR) be used to immediately record the receipt of money
- daily receipts totalling in excess of \$500 should be deposited the same day.

We observed that cheques received in the mail were opened by one Finance Officer. The Finance Officer recorded the mailed-in cheques immediately on the DRIR forms. The Finance Officer normally placed the DRIRs in a designated area for any of the Court Officers to process in FACTS as time permitted. Over the counter payments were immediately recorded in FACTS and a receipt was issued to the client by the Court Officer **(Schedule 1 refers)**.

At the end of the day, one of the two Finance Officers prepared the daily deposit. We noted that the daily deposit generally totalled over \$500 and was taken to the bank the next business day by the second Finance Officer.

We tested 80 transactions from the audit periods of both Trust Accounts and identified eight mailed-in cheques totalling \$342,860. These mailed-in cheques were not deposited between three and twenty-three calendar days after receipt. The individual value of the mailed-in cheques ranged from \$70 to \$102,690.

There was a risk that mailed-in cheques could go missing or be redirected to other accounts, accidentally or intentionally, if they were not processed in accordance with FAM.

**Risk Profile:**

<b>Risk Impact Level:</b>	Moderate: Requires specific allocation of management responsibility to ensure all monies get deposited on time.
<b>Risk Responsibility:</b>	Director, Finance & Administration, Justice
<b>Risk Mitigation Support:</b>	<ul style="list-style-type: none"><li>• Director, Court Services, Justice</li><li>• Administrator, NWT Courts, Justice</li></ul>

**Recommendation:**

We recommend that Court Registries comply with the requirements of FAM 2904 (415) Receipt and Deposit of Public Money.

**Management Response:**

<b>Action Plan</b>	<b>Completion Date:</b>
<i>Management agrees with this recommendation. Daily procedures will be developed to ensure compliance with FAM 2904 (415.)</i>	a) March 2017

#### 4. Disbursements to Creditors

##### Observation

Court Registries delayed over \$400,000 in Sheriff Trust account disbursements to clients by up to three months.

The *Creditors Relief Act* requires that money paid into Court by a debtor related to a writ order shall be distributed to the creditor within 14 days after Sheriff received the money. An option was available to extend the distribution for another 14 days by a judge.

From October 1, 2013 to January 31, 2016, Court Registries received over 1,800 incoming writ of execution (writ) payments. Court Registries receipted the incoming writ payments and deposited the money into the YK Court trust account. Management explained they were complying with the following Acts:

- *Judicator Act: Rules of the Supreme Court* section 531(1)(1.1), "... the garnishee shall pay into court..."
- *Creditors Relief Act* section 7, "Where money is paid into court under any garnishee proceedings, it shall be available for distribution by the Sheriff..."
- *Creditors Relief Act* section 9, "the Clerk shall, without an order, transfer to the Sheriff all money paid into court by virtue of a garnishee summons".

After the deposit, the Court Finance Officer would prepare a writ payment disbursement cheque from the YK Court trust account for deposit into the Sheriff Trust Account. After the deposit to the Sheriff Trust Account, the Sheriff Finance Officer would then process the disbursement to the creditor.

We tested 40 disbursements from the Sheriff Trust account and identified 17 writ disbursements. 11 out of the 17 writ disbursements in the audit sample, totalling \$474,088, did not comply with the *Creditors Relief Act* timelines and were delayed by as much as 100 days from the time of the second receipt by Court Registries. We noted that Court Registries:

- processed untimely deposits of mailed-in cheques **(Observation 3 refers)**
- repeated the receipt and deposit of cheques issued to the Sheriff trust account **(Schedule 1 refers)**

- used the FACTs data entry date of the Sheriff office writ payment as the receipt date not when the payment was actually received (**Schedule 1 refers**).

During the audit period, the duplicate manual processing of the 1,800 writ transactions by Court Registries delayed the settlement of the writs and did not provide relief for the creditor in a timely manner as required by the *Creditors Relief Act*. Court Registries reputation was at risk due to the internal procedures causing operational inefficiency and delay in managing court files.

**Risk Profile:**

<b>Risk Impact Level:</b>	Moderate: Requires specific allocation of management responsibility to ensure timely disbursement of money.
<b>Risk Responsibility:</b>	Director, Court Services, Justice NWT
<b>Risk Mitigation Support:</b>	<ul style="list-style-type: none"> <li>• Director, Finance &amp; Administration, Justice</li> <li>• Administrator, NWT Courts, Justice</li> </ul>

**Recommendation:**

We recommend that Court Registries redesign their process to comply with the:

- a) *Creditors Relief Act* disbursement requirements
- b) FAM 2904 (now 415) Receipt and Deposit of Public Money.

**Management Response:**

<b>Action Plan</b>	<b>Completion Date:</b>
<p>a) <i>Management agrees a review of the process will be helpful for documenting procedures for staff members and to ensure timely and efficient processing of disbursements. Management is currently engaging legal review of the authority to avoid the duplication between the Sheriff and Court Trust account and will revise this process accordingly if efficiencies are found.</i></p> <p>b) <i>Management agrees with this recommendation, processes will be updated accordingly.</i></p>	<p>a) June 2017 b) June 2017</p>



## 5. Accountable Forms Control

### Observation

Court Registries did not control accountable forms in accordance with FAM.

FAM 2905 Accountable Forms Control: All accountable forms must be prepared, distributed, issued, monitored, and accounted for.

We observed opportunities to strengthen internal controls by assigning responsibility for the custody and control of the following accountable forms:

- interim receipts used to receive cash from clients
- daily register of incoming revenue (DRIR) forms used to record the daily revenue received by Court Services
- blank cheques used to disburse funds from the trust accounts.

The weak internal controls of accountable forms would not allow management to detect accidental or intentional loss of cash or cheques. Delays in depositing the mailed-in cheques would be detected and corrected sooner if the reconciliation of DRIR forms and the receipts were conducted (**Observation 3 refers**).

### Risk Profile:

<b>Risk Impact Level:</b>	Minor: Requires management through specific, monitoring or response procedures.
<b>Risk Responsibility:</b>	Director, Finance & Administration, Justice
<b>Risk Mitigation Support:</b>	<ul style="list-style-type: none"><li>• Director, Court Services, Justice</li><li>• Administrator, NWT Courts, Justice</li></ul>

**Recommendation:**

We recommend that Court Registries comply with the requirements of FAM 2905 Accountable Forms Control.

**Management Response:**

<b>Action Plan</b>	<b>Completion Date:</b>
Management agrees with this recommendation.	March 31, 2017

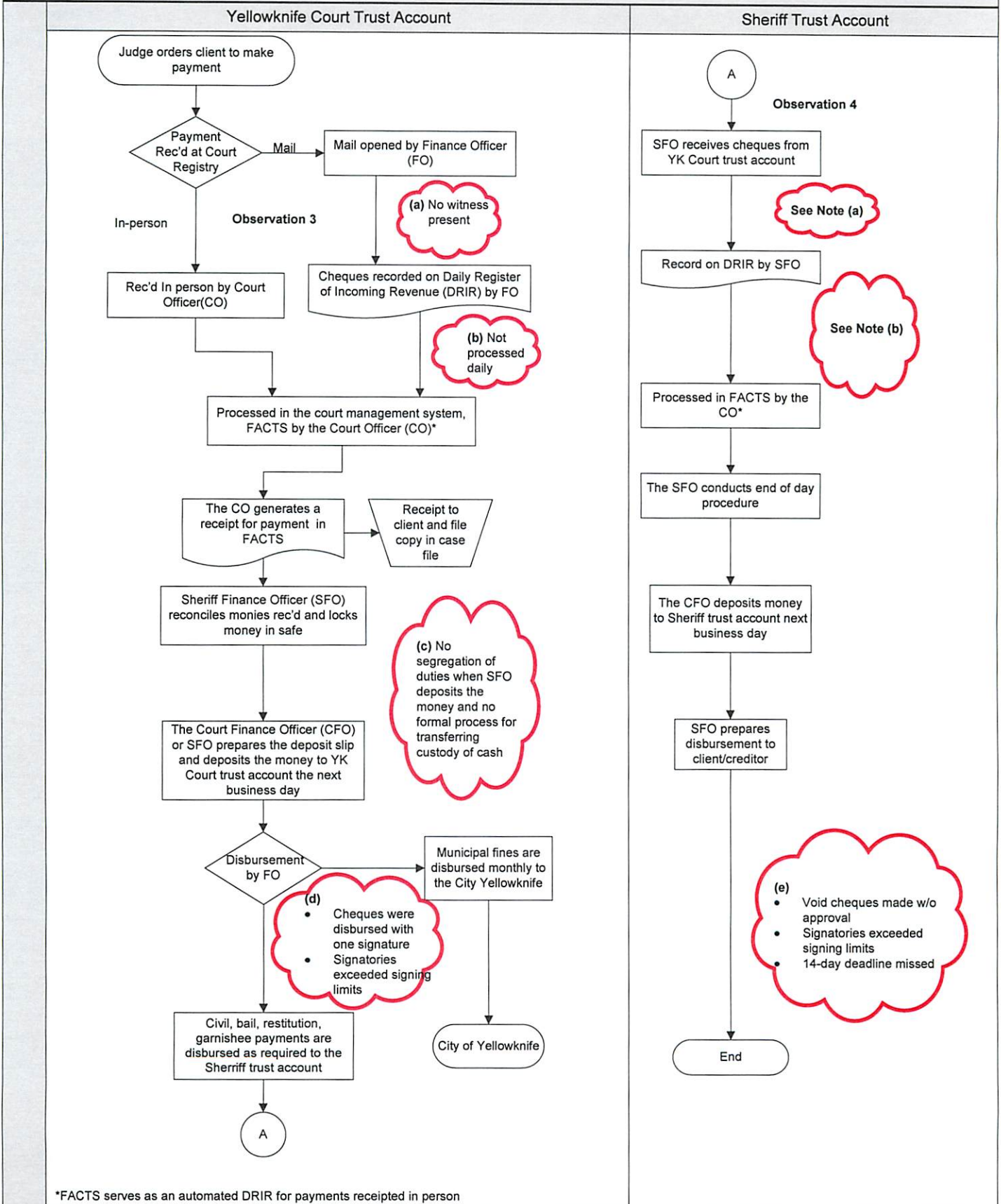
## E. ACKNOWLEDGEMENT

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

A handwritten signature in blue ink, appearing to read 'T. Bob Shahi', written in a cursive style.

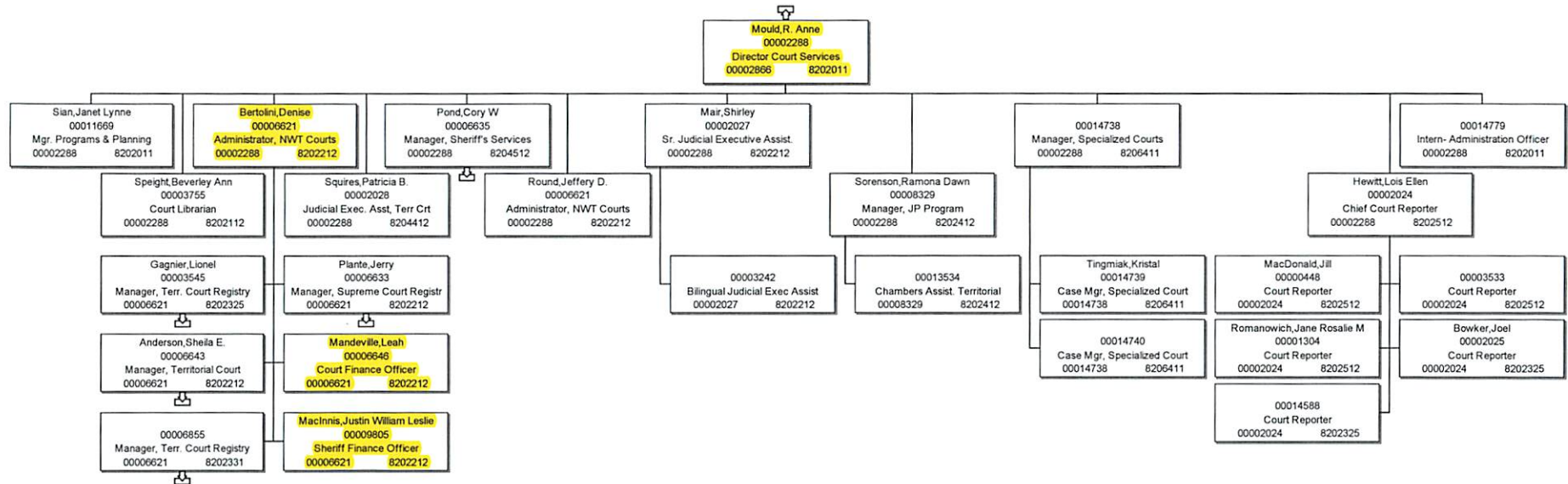
T. Bob Shahi  
Director

**Current:** Receipt, Deposit & Disbursement Process



Yellowknife Court and Sheriff Trust Accounts  
File: 7820-20-JUS-151-116 and 7820-20-JUS-151-117

APPENDIX A





MAY 11 2018

**CONFIDENTIAL**

File: 7820-20-GNWT-151-131

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**Access to Information and  
Protection of Privacy Assessment, Corporate Privacy Risk Assessment**

Enclosed is the above referenced Corporate Privacy Risk 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 December 2018 on the status of the management action plan.

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. Mandi Bolstad, Director, Corporate Services, Justice



## JUSTICE

Access to Information and Protection of Privacy,  
Corporate Privacy Risk Assessment

Internal Audit Bureau

May 2018



## **JUSTICE**

### **Access to Information and Protection of Privacy, Corporate Privacy Risk Assessment**

**May 2018**

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





**CONFIDENTIAL**

May 11, 2018

File: 7820-20-GNWT-151-131

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**Audit Report: Access to Information and Protection of Privacy, Corporate Privacy Risk 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 with a focus on the privacy of information.

In assessing the privacy of information for the departments, a number of recommendations impacted more than one department. This report summarizes those items.

**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 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 to comply with the *ATIPP Act*.

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

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

### C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached audit report, *“Corporate Privacy Report – ATIPP Privacy of Information”*, made a number of observations and recommendations impacting more than one department

The contractor assessed the compliance with the *ATIPP Act* and Regulations. There was lack of compliance or information was not available for verification in all departments except one (EIA). However, with the exception of one department, most of the non-compliance impacted only one or two areas of the *ATIPP Act* or Regulations.

The contractor also assessed the capacity (maturity rating) of nine privacy principles for all departments. Overall, the privacy risk for departments ranged from “very low” to “very high” (**Chart I Refers**). This was expected as each department has a unique mandate and need to access diverse information for program delivery:

- Five departments had “high” to “very high” risk
- Three departments had “medium” risk.
- Three departments had “low” to “very low” risk

Majority of the departments did not have the internal control capacity to address the privacy risk (**Chart I Refers**). With the exception of two departments with “very low” risk, the other eight departments would need to build their internal control capacity to address the assessed privacy risk. The internal control capacities for departments were assessed at either the “ad-hoc” or “repeatable” level. This capacity would be appropriate for “low” to “very low” risk levels. The immediate task for most departments was to document privacy processes (defined level). Subsequently, departments 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 included:

- Creating a GNWT Wide privacy policy and an associate guidance for use by departments.
- Co-ordinating training on privacy through APO.
- Monitoring of compliance with ATIPP.
- Completing inventory of personal information collected and stored.

An Executive Management decision for GNWT will be required to determine the criteria used to allocate limited resources: "Compliance" vs. "Risk". In some instances, the privacy risk does not warrant additional internal controls. However, to be compliant with *ATIPP Act*, departments may have to allocate resources (i.e. Lands). Conversely, some departments need to go beyond compliance to fully address the privacy risk (i.e. - ECE).

The management response to the contractor's recommendations was co-ordinated by APO. The IAB will follow-up on the status of the management action plan after six months during our scheduled follow-up audits.

The implementation of the draft "*Protection of Privacy Policy*" and the "*Guidelines for Privacy Management Program*" will be the key in addressing the privacy risks in the GNWT environment.

#### **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

**Risk and Opportunity Assessment using Capacity Model**

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

		Internal Control Capacity Level				
		Ad-hoc	Repeatable	Defined	Managed	Optimized
<b>Privacy Risk Level</b>	Very High	<b>ECE</b>	<b>Justice H&amp;SS</b>			
	High	<b>Finance INF</b>				
	Medium	<b>ENR</b>	<b>ITI</b>			
	Low	<b>MACA</b>				
	Very Low	<b>Lands</b>	<b>EIA</b>			

	Range where Risk and Internal Control Capacity Level match.
	Inadequate capacity to address privacy risk
	Resources used to build capacity for compliance but unnecessary to address privacy risk



## Table of Contents

- Crowe MacKay Corporate Privacy Report
  - Schedule 1
  - Schedule 2
  - Appendix A
- Appendix B - Justice
- Appendix C – Education, Culture and Employment
- Appendix D – Executive and Indigenous Affairs
- Appendix E – Environment and Natural Resources
- Appendix F - Finance
- Appendix G – Health And Social Services
- Appendix H - Infrastructure
- Appendix I – Industry, Tourism and Investment
- Appendix J – Lands
- Appendix K – Municipal and Community Affairs



**Government of the Northwest Territories  
Corporate Privacy Report – ATIPP Privacy of Information**

**Date:** April 30, 2018  
**To:** **Bob Shahi**, Director, Internal Audit Bureau, Government of the Northwest Territories  
**From:** 23(2)(d) [REDACTED] Advisory Services, Crowe MacKay LLP  
**Re:** Corporate Privacy Report – ATIPP Part 2 Compliance as at March 31, 2018

---

## **A. 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), the successful proponent, coordinated all work directly under the supervision of the Director, Internal Audit Bureau.

Testing of departments was undertaken based on the Generally Accepted Privacy Principles (GAPP) (**Schedule 1 refers**) to determine risk and compliance by each department included in our scope. Fieldwork was also undertaken in accordance with the Institute of Internal Auditors guidance on risk-based internal auditing as a methodology that links internal auditing to an organization’s overall risk management framework.

During the week of February 5, Crowe MacKay conducted initial meetings with both the Internal Audit Bureau (IAB) as well as the Access and Privacy Office (APO) to identify the current state of compliance by the GNWT with Part 2: Protection of Privacy in order to undertake an initial assessment of the maturity of the control environment as designed and implemented. During these meetings it was discovered that compliance was less mature than expected. Considering that a less mature control environment may be in place across the 10 departments indicated within the scope of our engagement, we adjusted our focus to be less compliance-based and more risk-based with a strong focus on the maturity levels denoted in the Privacy Maturity Model (PMM) as developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) (**Appendix A refers**).

Crowe MacKay relied less on substantive testing of controls and rather addressed the risks related to effectively establishing a sound governance framework by the APO as well as how each department interpreted this framework for departmental application.

The scope of this engagement excluded the NWT Housing Corporation, the other 22 public bodies noted in the Act’s Regulations, the Health Information Act, and the Office of the Legislative Assembly. The Office of the Legislative Assembly is not included in the definition of a “public body” as per Section 2 of ATIPP and is therefore exempt from most aspects of this legislation.

## **B. BACKGROUND**

In December 1996, the Legislative Assembly of the Northwest Territories passed the Access to Information and Protection of Privacy Act. The Act plays a critical role in maintaining government accountability and protecting the public’s personal information. The Act is comprised of two separate parts:

1. **Part 1: Access to Information:** Provides the public with a process to obtain access to most records in the possession or control of public bodies.
2. **Part 2: Protection of Privacy:** Provides guidance to the GNWT for when and how its public bodies can collect personal information, what they can use such information for once it has been collected, and in what situations the information can be disclosed to another public body or the general public.

ATIPP gives the public the right to request access to their own personal information held by Northwest Territories' public bodies as well as the right to request a correction to that same personal information. The legislation also sets out when a public body may collect, use and disclose personal information.

ATIPP further provides for an independent review by the NWT Information and Privacy Commissioner (IPC) of the decisions made under the Act. The Commissioner may also review how a public body has collected, used or disclosed personal information. The IPC is an Officer of the Legislature and reports directly to the Legislative Assembly of the Northwest Territories. The IPC is independent of the government of the day.

The APO recognizes and applies GAPP which also form part of the GNWT Privacy Management Framework. These principles are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. GAPP principles are supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance. This audit leveraged these principles to both assess the current control environment for the protection of privacy as well as to provide a maturity rating against the PMM.

The PMM is 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.

In developing the PMM, it was recognized that each organization's personal information privacy practices may be at various levels of maturity. It was also recognized that, based on an organization's approach to risk, not all privacy initiatives would need to reach the highest level in the maturity model. Each of the GAPP criteria are broken down according to the five maturity levels (Ad Hoc, Repeatable, Defined, Managed or Optimized) as outlined in the PMM. This allows entities to obtain a picture of their privacy program or initiatives both in terms of their status and, through successive reviews, their maturation.

## C. DEPARTMENTAL OVERVIEW

The 10 departments were reviewed using interviews and detailed review of documents to support controls noted to be in place. An assessment of each department's compliance with the ATIPP Part 2 legislation was made as well as an assessment of their current level of maturity in relation to the PMM. Although the review was performed from a risk-based perspective, it was also determined that a basic level of compliance should be met in relation to ATIPP Part 2 in order for information to be adequately protected.

The following three pages outline the overviews for the departments. The first contains a chart showing compliance with each area of legislation in ATIPP Part 2. The second shows the level of maturity that each department had obtained in relation to each of the GAPP Principles. The third outlines the level of maturity in relation to the significance of the risk of the data held by each department. Specific findings relating to the legal obligations and maturity levels can be found in the attached departmental reports.

## Legal Obligations Departmental Overview

As assessment of each department’s compliance with legal obligations under ATIPP Part 2 (**Schedule 2 refers**) was made. Department compliance is outlined in the chart below by legislative area.

**Legend:**

- C** Compliant;
- NC** Non-Compliant
- N/A** Not Applicable (refer to full report for department for reasoning)
- UV** Unverified

Clause	ECE	ENR	EIA	FIN	HSS	INF	ITI	DOJ	LANDS	MACA
40	C	C	C	C	C	C	C	C	C	C
41(1)	NC	C	C	C	C	C	C	C	C	C
41(2)&(3)	NC	NC	C	NC	C	NC	C	C	NC	NC
42	NC	C	C	C	C	C	C	C	C	C
43	NC	C	C	C	C	C	C	C	C	C
44	NC	C	C	C	C	C	C	C	C	C
45	C	NA	NA	C	NA	NA	NA	NA	C	C
46	NA	NA	NA	C	NA	NA	NA	NA	NA	C
47	UV	C	NA	C	C	UV	C	C	C	UV
47.1	UV	UV	NA	UV	UV	UV	UV	UV	UV	UV
48	NC	UV	NA	C	UV	C	C	C	C	UV
49	NC	NC	NA	N/A	NA	C	N/A	C	NA	NA
5(REG)	NC	C	C	C	C	C	C	C	C	C
6(REG)	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
8(REG)	UV	NA	NA	NA	NA	C	NA	NA	NA	NA



## Maturity Rating against Privacy Maturity Model – Departmental Overview

The GNWT Access and Privacy Office recognizes and applies GAPP which also forms part of the GNWT Privacy Management Framework. These GAPP principles are supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance. The GAPP principles are essential to the proper protection and management of personal information. They are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

Based on the audit work performed, an understanding of the current control environment for the protection of privacy in each department was developed which was used to provide a maturity rating for each principle of GAPP, (excluding access) using the PMM (Appendix A refers). The assessed maturity across the departments is illustrated in the graph below. Departments have been provided with steps to be taken for them to achieve the minimum maturity level required. However, due to the risk of data held within certain departments, it is recommended that additional planning be taken by those departments to reach a higher level of maturity within the privacy control environment.

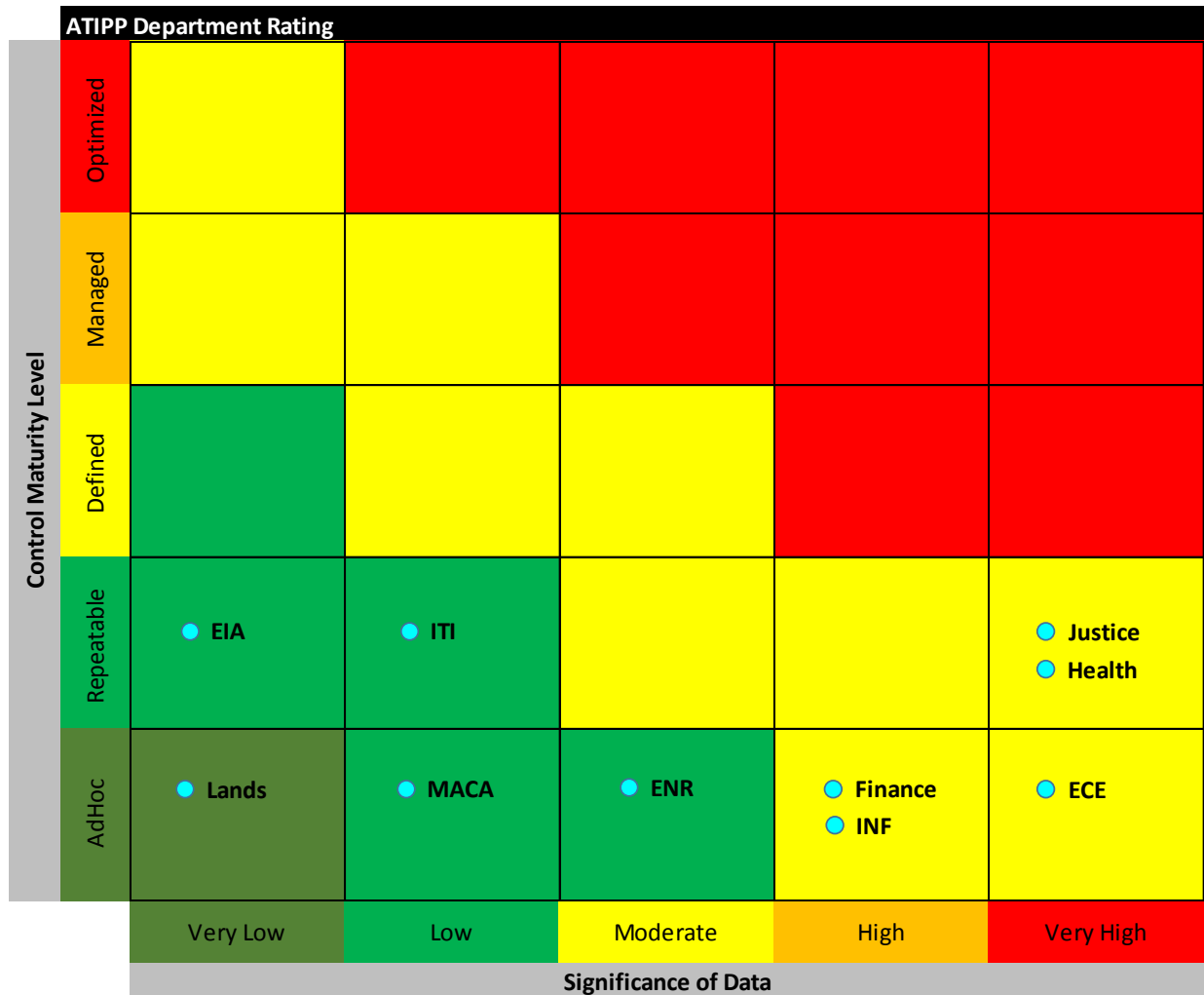
**Legend:**

- 1 Ad Hoc
- 2 Repeatable
- 3 Defined
- 4 Managed
- 5 Optimized

Maturity Model Principle	ECE	ENR	EXEC	FIN	HEA	INFR	ITI	DOJ	LANDS	MACA
<b>MANAGEMENT</b>	1	1	2	2	2	2	1	2	1	1
<b>NOTICE</b>	1	1	3	1	3	1	3	3	1	1
<b>CHOICE AND CONSENT</b>	1	1	3	1	2	1	3	3	2	1
<b>COLLECTION</b>	1	1	2	2	2	2	2	2	1	1
<b>USE, RETENTION &amp; DISPOSAL</b>	1	2	2	2	2	1	2	2	2	2
<b>DISCLOSURE TO THIRD PARTIES</b>	1	1	NA	1	2	2	2	2	1	1
<b>SECURITY FOR PRIVACY</b>	1	2	2	2	2	2	2	2	1	1
<b>QUALITY</b>	1	1	2	2	2	1	2	2	1	1
<b>MONITORING AND ENFORCEMENT</b>	1	1	1	1	1	1	1	2	1	1

## Departmental Risk Assessment

Each department was assessed based on its control environment for compliance with ATIPP as well as the overall number of records and significance/sensitivity of the records held. This rating is plotted on the chart below and was used to determine to what level of maturity a department should reach in order to adequately protect the data for which it was responsible.



## D. OBSERVATIONS AND RECOMMENDATIONS

The APO resides within the Department of Justice of the GNWT. However, the APO has responsibility to provide guidance on the establishment of the governance framework for ensuring departments within the GNWT both design and implement a control environment suitable for ongoing compliance with all aspects of ATIPP. Government-wide observations are included below which are to be addressed at the corporate level for setting expectations across all departments, including providing training, policies, procedures and manuals where required. Separate department-specific observations are included in the appendices to this report. These observations have been presented in order of risk, from highest to lowest.

## Department Comments

We would note that in relation to risk responsibility, the ATIPP legislation clearly indicates responsibility for the protection of personal information rests directly with the head of each individual public body. (Section 42 ATIPP Act). Therefore the risk responsibility in relation to the protection of personal information does not fall under the responsibility of the Department of Justice.

However, as we have noted in the responses below, the GNWT Protection of Privacy Policy and the Guidelines for Privacy Management Program was developed to support and advise departments in relation to the protection of personal information in their custody or control, and is intended to better equip departments to meet the privacy requirements of the Act.

### Observation 1

**A Government-wide privacy policy (including guidance documentation) in relation to ATIPP Part 2 is not yet in place**

- Draft documentation has been created but has yet to be finalized for release as guidance to all departments.
- The responsibility and authority to develop the privacy policy is unclear (i.e. APO or department).

### Risk Profile:

Risk Impact	Lack of a consistent policy at the GNWT level has led to confusion and extremely varied responses to ATIPP legislation compliance at the department level
Risk Responsibility	DM Department of Justice
Risk Mitigation Support	Access and Privacy Office employees

### Recommendations:

We recommend that:

- The APO develop a Government-wide privacy policy and associated guidelines/manual for prescriptive application within each department where compliance has been delegated.
- This one policy should address requirements as set out within ATIPP and to ensure the privacy principles are sufficiently addressed to meet minimum maturity requirements.
- Departments should not be attempting to interpret legislation on an ad hoc basis but rather should be developing processes to meet the policy and guidelines as established by the APO.

### Management Response:

Action Plan:	Completion Date:
<p>The Department of Justice, APO has drafted a GNWT Protection of Privacy Policy and Guidelines for Privacy Management Program, which has been shared with all departments for review and discussion.</p> <p>The Policy is expected to be finalized by June 30, 2018 with implementation throughout the GNWT commencing shortly thereafter.</p>	Fall 2018

The GNWT Protection of Privacy Policy and Guidelines for Privacy Management Program is intended to assist GNWT departments in implementing ATIPP requirements in relation to protection of personal information. However, a suitable period of time (i.e. at least 1 year) will be needed for implementation.	Fall 2019
We agree that it is important that there is a consistent application of the legislation, by departments, in relation to the protection of personal information. In fact, this consistency is one of the desired outcomes of the GNWT Privacy Framework and Management Program which is currently under development and scheduled for implementation in 2018.	Fall 2018

## Observation 2

### Current training for ATIPP is not adequate

- Although there is online ATIPP training available for government employees, this is not required.
- The three day intensive ATIPP training for coordinators is not offered on a regular basis to meet the needs of the departments audited during this engagement.
- Departments are either are not aware of or are not required to complete an online training course related to IT security.

### Risk Profile:

Risk Impact	Lack of training reduces the likelihood of building a “culture” of privacy compliance, and also increases the risk of ATIPP non-compliance, both directly and indirectly
Risk Responsibility	DM Department of Justice
Risk Mitigation Support	Access and Privacy Office employees

### Recommendations:

We recommend that:

- Both the ATIPP and IT Security training which is available online should be made mandatory for employees accessing or obtaining personal information.
- Intensive training be offered on a regular schedule to meet the varying needs of each department.

### Management Response:

Action Plan:	Completion Date:
As part of the roll out of the GNWT Protection of Privacy Policy and Guidelines for Privacy Management Program, the APO will work with Departments to identify program employees who would benefit from taking the online privacy and security training.	May 2019

<p>However, we do not believe mandatory training is currently required at this time.</p>	
<p>The Department of Justice recognizes public bodies benefit from training opportunities relating to protection of personal information. As a result, privacy training is a major component of the GNWT Privacy Framework and Management Program.</p> <p>The proposed GNWT Guidelines for Privacy Management Program outline the Department of Justice’s commitment to provide training to GNWT staff who have been identified by their respective department.</p> <p>However the pace of training must be delivered within the scope of the existing resources of the APO.</p>	<p>May 2019</p>

### Observation 3

**Monitoring of compliance with ATIPP is not fully performed**

- The APO does not have a clearly laid out and documented process for monitoring departments to ensure their compliance with ATIPP.
- Departments are not required to complete any kind of self-assessment in relation to protection of privacy and their compliance with ATIPP Part 2 legislation.

#### Risk Profile:

Risk Impact	Lack of monitoring increases the risk of non-compliance with ATIPP
Risk Responsibility	DM Department of Justice
Risk Mitigation Support	Access and Privacy Office employees

#### Recommendations:

We recommend that:

- A monitoring program be developed and implemented which ensures a regular review of compliance is done in relation to all departments.
- A process be put into place whereby departments complete a yearly self-assessment regarding their ATIPP compliance and submit it to the APO for review.

#### Management Response:

Action Plan:	Completion Date:
<p>ATIPP legislation clearly indicates responsibility for the protection of personal information rests directly with the head of each individual public body (Section 42 ATIPP Act).</p>	<p>N/A</p>

<p>Therefore the Department of Justice has no authority to monitor compliance by public bodies subject to the Act.</p> <p>However the GNWT Privacy Framework and Management Program was developed to support and advise departments in relation to the protection of personal information in their custody or control, and is intended to better equip departments to meet the privacy requirements of the Act.</p>	
<p>The GNWT recognizes the importance of assessing departmental privacy programs. Therefore the GNWT Privacy Framework and Management Program includes a privacy audit self-assessment tool that will allow a department to assess the status of their departmental privacy program.</p> <p>The APO, however, is recommending that the self-assessments take place every two years.</p>	<p>May 2020</p>

#### Observation 4

**Archival-selected records held by NWT archives, which may contain personal information, are not fully secure and some records which belong in the archives cannot be obtained**

- There are concerns regarding the security of archived records and the ability of staff to manage the volume of records.
- Archiving responsibilities reside within Education, Culture and Employment (ECE) but the duties are Government-wide, and records from all areas are stored here.
- Items flagged in DIIMS for archive cannot be moved to the archives as there is no method in place to transfer the files.

#### Risk Profile:

Risk Impact	If records selected for storage in NWT archives are not fully protected and files are not moved into correct stages of archiving to a safe and secure location, there is in increased risk of non-compliance with ATIPP
Risk Responsibility	Corporate Information Management Office out of INF
Risk Mitigation Support	Access and Privacy Office employees, archival staff members

#### Recommendations:

We recommend that:

- A review of the archiving facilities, processes and staffing should take place to ensure that sufficient resources are employed to support the protection of personal information stored in these locations.

- A method of transferring documents flagged for archive from DIIMS to the archival system be developed.

**Management Response:**

Action Plan:	Completion Date:
<p>CIM has set a meeting with the NWT Archives and the APO, for May 2, 2018, to discuss the NWT Archives temporary physical storage space, currently provided for them in the Yellowknife Record Storage Center.</p> <p>The discussion will include identifying the responsibilities related to the protection of personal information in records held by the NWT Archives and the necessary steps required to address this issue.</p>	May 2019
<p>CIM developed and implemented a disposition process in the DIIMS to flag and transfer records identified for Archival Selection to the NWT Archives.</p> <p>Archives requirements for digital transfer include adherence to appropriate standards, middleware for transfer, archival systems for digital ingest and processing of government records and an archivally-sound trusted digital repository. Without these systems in place to receive records in an archivally-sound manner, transfer cannot occur.</p> <p>Both CIM and the NWT Archives will meet in June 2018, to discuss. However it must be recognized that the solution to address this issue will require significant resources, which may not be currently available.</p>	September 2019

**Observation 5**

**There is a lack of clarity as to whether or not Information Sharing Agreements are required between departments**

- Currently there is confusion both within and amongst the departments as to whether or not Information Sharing Agreements are required for information being shared between GNWT departments.

**Risk Profile:**

Risk Impact	Lack of clarity in this area has resulted in varying processes being used in each departments and inconsistency in use of agreements. This increases the risk that ATIPP compliance may not be in place
Risk Responsibility	DM Department of Justice

Risk Mitigation Support	Access and Privacy Office employees
-------------------------	-------------------------------------

**Recommendations:**

We recommend that:

- GNWT assess whether ATIPP legislation requires inter-departmental sharing of personal information to be covered off by an Information Sharing Agreement.
- GNWT develop clear guidelines based on the assessment above to ensure that all departments know when they do and do not require an Information Sharing Agreement.

**Management Response:**

Action Plan:	Completion Date:
The GNWT Protection of Privacy Policy and Guidelines for Privacy Management Program will require the use of Personal Information Sharing Agreements (PISA). The PISA guideline and template will be finalized as part of the overall GNWT Privacy Framework and will assist departments in assessing when a PISA is required.	Fall 2019
The PISA guidelines identify that any sharing of personal information between public bodies or a public body and another other entity should be addressed in a personal information sharing agreement.	Fall 2019

**Observation 6**

**Departments do not all have a clear understanding of the point at which their responsibility for ATIPP ends and that of smaller public bodies begins.**

- Departments are incurring costs for compliance with Part 2 in situations where the cost of compliance should be carried by another public body. This is due to confusion as to who will be held responsible if personal information is exposed.

**Risk Profile:**

Risk Impact	There is an increased risk that documents that are insecure may not be dealt with due to role confusion, or that funds from one budget may be used for work that does not fall under the purview of that department.
Risk Responsibility	DM Department of Justice
Risk Mitigation Support	Access and Privacy Office employees

**Recommendations:**

We recommend that:

- Clear guidelines be established to address which responsibilities apply between departments and smaller public bodies with respect to personal information within their custody. Although the legislation clearly identifies the different entities, having guidance in place to state that responsibility for



compliance also falls along those lines would allow departments to draw the line in relation to work being done and to be clear about what documents they are not responsible for.

- This must come from a government directive to ensure clarity at the department level.

**Management Response:**

Action Plan:	Completion Date:
<p>In the Department of Justice’s review of this matter, we believe the ATIPP legislation clearly identifies that public bodies identified in the Regulations, are considered separate entities under the ATIPP Act, and, any functions of the Act, relating to either access to information and/or the protection of personal information is the responsibility of the designated head of the public body, not with a GNWT Department.</p> <p>As this is outlined in the legislation, and the roles and responsibilities of public bodies in relation to the Act is being addressed in the ATIPP Policy and Guidelines Manual, no GNWT guideline or directive is required.</p>	<p>N/A</p>
<p>See Above</p>	<p>N/A</p>

# SCHEDULE 1

## GENERALLY ACCEPTED PRIVACY PRINCIPLES (GAPP)

The table below outlines the 10 Generally Accepted Privacy Principles that have been developed by the CICA and AICPA to assist organizations in strengthening their privacy policies as discussed in the AICPA/CICA Privacy Maturity Model User Guide (Appendix A).

Principle	Description
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.

## SCHEDULE 2

### LEGAL OBLIGATIONS CLAUSE DESCRIPTIONS

Clause #	Description
40	Are you collecting personal information: <ul style="list-style-type: none"><li>• is it authorized by law? (if yes, what law)</li><li>• is it collected for the purpose of law enforcement?</li><li>• is it necessary for an existing program or activity?</li><li>• has the DM and Cabinet authorized collection for a proposed program or activity?</li></ul>
41(1)	Is the personal information collected directly from the individual?
42(2) and (3)	If you are collecting information directly from an individual, have you told them: <ul style="list-style-type: none"><li>• why you are collecting the information</li><li>• the legal authority for collecting the information</li><li>• the title address and phone number of someone who can answer questions about the collection</li></ul>
42	No legal obligation beyond making reasonable security arrangements to protect personal information against risks such as unauthorized access, collection, use, disclosure or disposal
43	If you are using personal information is it for: <ul style="list-style-type: none"><li>• the purpose for it which it was collected</li><li>• or has the person consented in writing to the specific use of the information or to whom the information is being disclosed</li></ul>
44	If you are using the personal information to make a decision that directly affects that individual, have you <ul style="list-style-type: none"><li>• made every reasonable effort to ensure the information is accurate and complete</li></ul>
45	If an individual has identified an error or omission and requested a correction, have you: <ul style="list-style-type: none"><li>• within 30 days let them know that the correction has been made or whether it has been refused</li></ul> If the correction is refused, have you: <ul style="list-style-type: none"><li>• made note of the correction requested and the refusal to correct on the record storing the personal information?</li></ul>
46	If the personal information that is the subject of a request for correction, has been disclosed to another public body or third party within the previous 12 months, have you: <ul style="list-style-type: none"><li>• notified the recipient that the personal information was corrected or that a request for correction was refused</li></ul> If you receive a notification that personal information was corrected, have you: <ul style="list-style-type: none"><li>• made a correction to the personal information in any records you hold</li></ul>
47	If you are disclosing information, is it in accordance with the access to information provisions of the Act, or Division C of the Act?

## SCHEDULE 2

### LEGAL OBLIGATIONS CLAUSE DESCRIPTIONS

Clause #	Description
47.1	An employee can not disclose personal information received in the course of their duty without authorization.
48	<p>Personal information should not be disclosed UNLESS:</p> <ul style="list-style-type: none"> <li>• it is disclosed for the purpose for which it was collected, or a use consistent with that purpose</li> <li>• the individual has consented in writing to the disclosure of the information for that purpose or to whom the information is being disclosed to</li> <li>• it is to enforce a legal right the Government has against that person (if yes, what legal right)</li> <li>• it is for the purpose of collecting a fine or debt owed to the Government</li> <li>• it is for the purpose of making a payment owed to an individual by the Government</li> <li>• for law enforcement purposes</li> <li>• the Minister of Justice or their agent or lawyer is disclosing the information to persons responsible for a place of lawful detention</li> <li>• the information is used for the hiring, managing or administering the employees of the Government</li> <li>• it is to the Maintenance Enforcement Administrator for the purpose of enforcing child support under that Act</li> <li>• it is to the Information and Privacy Commissioner in the course of her duties</li> <li>• it is to the Auditor General of Canada or the Internal Audit Bureau for audit purposes</li> <li>• to an employee of the Government or to a Cabinet member where they need the information to perform their duties</li> <li>• it is being used to provide legal services to the Government</li> <li>• it is being disclosed to the Northwest Territories Archives for archival purposes</li> <li>• disclosure is required because of a valid subpoena or warrant</li> <li>• it is for the purpose of supervising an individual under the supervision of a correctional authority</li> <li>• it is required to protect the mental or physical health or safety of any individual</li> <li>• it is for the purpose of contacting the next of kin of an injured, ill or deceased individual</li> <li>• in the opinion of the Deputy Minister, the public interest in disclosure outweighs the invasion in privacy, or disclosure benefits the individual whose information it is</li> <li>• the information is already available to the public</li> <li>• it is in accordance with a law (if yes, which law)</li> <li>• it is to an MLA who can show that the individual whose information it is has requesting their assistance in solving a problem</li> </ul>
49	<p>The disclosure of personal information for research or statistical purposes is prohibited UNLESS:</p> <ul style="list-style-type: none"> <li>• the research cannot reasonably be accomplished unless information is presented in a form that allows individual information can be identified</li> <li>• the disclosure of the information is not harmful to the individual and the benefit from disclosure is in the public interest</li> </ul>

## SCHEDULE 2

### LEGAL OBLIGATIONS CLAUSE DESCRIPTIONS

Clause #	Description
	<ul style="list-style-type: none"><li>the Deputy has approved conditions for the release relating to security and confidentiality of the information, the removal or destruction of identifying information, and a prohibition on the further release of information without the Government's consent and the researcher has signed an agreement to these conditions that complies with the regulations (<i>Section 8 of the Regulations</i>).</li></ul>
6	Personal information may be disclosed to an employee or Government contractors in order to carry out a formal examination of a government program or a part of program IF that examination is authorized by law or public policy.
8	<p>If you are disclosing personal information under a research agreement, that agreement must include:</p> <ul style="list-style-type: none"><li>a condition that the information can only be used for the purpose set out in the agreement, or in the written authorization they have received from the government</li><li>the identity of any other person who may be given access to the information</li><li>a condition that the researcher will enter into a similar agreement with any other person who may be given access to the information</li><li>a condition to keep the information in a secure location that restricts access to the information</li><li>a condition had the research remove or destroy individual identifying information by a set date in a specified manner</li><li>a condition that the researcher must not contact anyone whose information they receive without written consent of the government</li><li>a condition that</li><li>the information is not used for any administrative purpose that affects the individual whose information it is</li><li>a requirement that the researcher notify the government of any breach of the terms of the agreement;</li><li>a requirement that the agreement may be terminated if the researcher breaches the agreement</li></ul>

# **APPENDIX A**

## **MATURITY MODEL**

# 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](http://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 Federer

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

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

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](http://www.aicpa.org/privacy) and [www.cica.ca/privacy](http://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 Model<sup>1</sup> 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.

<sup>1</sup> 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

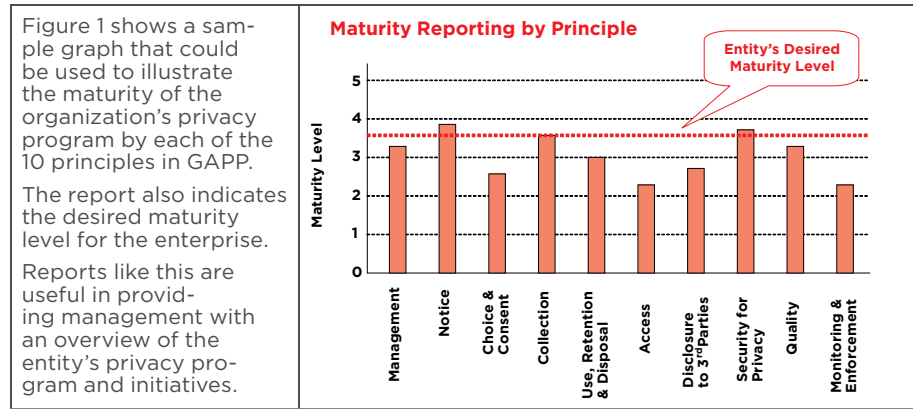


Figure 2 - Maturity Report by Criteria within a Specific GAPP Principle

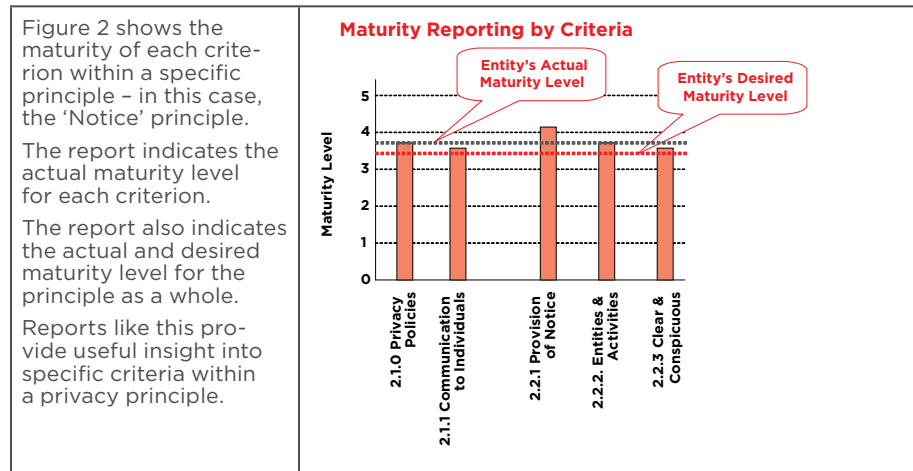
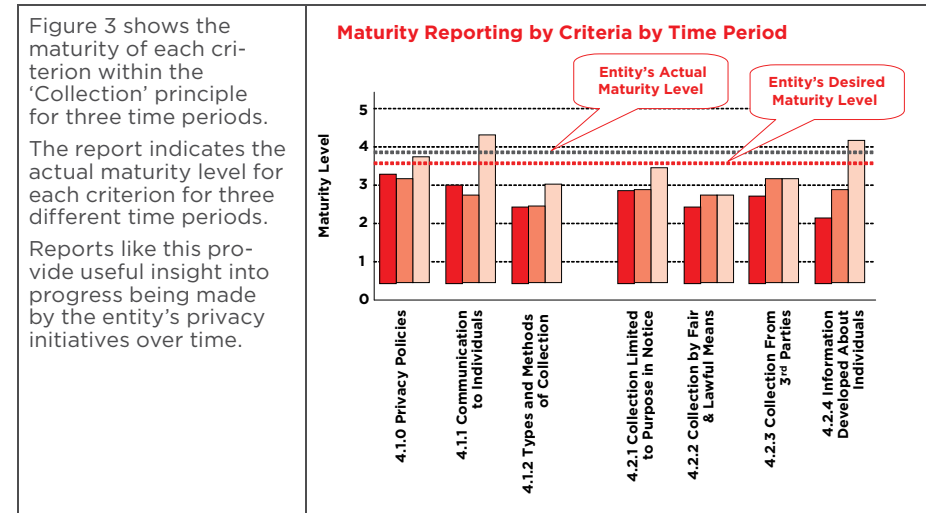


Figure 3 - Maturity Report by Criteria within a GAPP Principle Over Time



## 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 MODEL<sup>1</sup>

## Based on Generally Accepted Privacy Principles (GAPP)<sup>2</sup>

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria)</b>	<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>					
<b>Privacy Policies (1.1.0)</b>	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.
<b>Communication to Internal Personnel (1.1.1)</b>	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.

<sup>1</sup> 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.

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

GAPP - 73		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Responsibility and Accountability for Policies (1.1.2)</b>	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.
<b>Review and Approval (1.2.1)</b>	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.
<b>Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Personal Information Identification and Classification (1.2.3)</b>	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.
<b>Risk Assessment (1.2.4)</b>	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.
<b>Consistency of Commitments with Privacy Policies and Procedures (1.2.5)</b>	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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Infrastructure and Systems Management (1.2.6)</b>	<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"> <li>• Infrastructure</li> <li>• Systems</li> <li>• Applications</li> <li>• Web sites</li> <li>• Procedures</li> <li>• Products and services</li> <li>• Data bases and information repositories</li> <li>• Mobile computing and other similar electronic devices</li> </ul> <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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Privacy Incident and Breach Management (1.2.7)</b>	<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"> <li>• Procedures for the identification, management and resolution of privacy incidents and breaches</li> <li>• Defined responsibilities</li> <li>• A process to identify incident severity and determine required actions and escalation procedures</li> <li>• A process for complying with breach laws and regulations, including stakeholder breach notification, if required</li> <li>• An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate</li> <li>• 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"> <li>– Incident patterns and root cause</li> <li>– Changes in the internal control environment or external requirements (regulation or legislation)</li> </ul> </li> <li>• Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed</li> </ul>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Supporting Resources (1.2.8)</b>	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.
<b>Qualifications of Internal Personnel (1.2.9)</b>	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.
<b>Privacy Awareness and Training (1.2.10)</b>	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
<b>MANAGEMENT (14 criteria) cont.</b>		<b>The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</b>				
<b>Changes in Regulatory and Business Requirements (1.2.11)</b>	<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"> <li>— Legal and regulatory</li> <li>— Contracts, including service-level agreements</li> <li>— Industry requirements</li> <li>— Business operations and processes</li> <li>— People, roles, and responsibilities</li> <li>— Technology</li> </ul> <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.
<b>NOTICE (5 criteria)</b>		<b>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</b>				
<b>Privacy Policies (2.1.0)</b>	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.
<b>Communication to Individuals (2.1.1)</b>	<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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>NOTICE (5 criteria) cont.</b>	<b>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</b>					
<b>Provision of Notice (2.2.1)</b>	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).
<b>Entities and Activities Covered (2.2.2)</b>	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.
<b>Clear and Conspicuous (2.2.3)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria)</b>		<b>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.</b>				
<b>Privacy Policies (3.1.0)</b>	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.
<b>Communication to Individuals (3.1.1)</b>	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.
<b>Consequences of Denying or Withdrawing Consent (3.1.2)</b>	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		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria) cont.</b>	<b>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.</b>					
<b>Implicit or Explicit Consent (3.2.1)</b>	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.
<b>Consent for New Purposes and Uses (3.2.2)</b>	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.
<b>Explicit Consent for Sensitive Information (3.2.3)</b>	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		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>CHOICE and CONSENT (7 criteria) cont.</b>	<b>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.</b>					
<b>Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices (3.2.4)</b>	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.
<b>COLLECTION (7 criteria)</b>	<b>The entity collects personal information only for the purposes identified in the notice.</b>					
<b>Privacy Policies (4.1.0)</b>	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.
<b>Communication to Individuals (4.1.1)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>COLLECTION (7 criteria) cont.</b>		<b>The entity collects personal information only for the purposes identified in the notice.</b>				
<b>Types of Personal Information Collected and Methods of Collection (4.1.2)</b>	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.
<b>Collection Limited to Identified Purpose (4.2.1)</b>	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"> <li>• be fully documented;</li> <li>• distinguish the personal information essential for the purposes identified in the notice;</li> <li>• differentiate personal information from optional information.</li> </ul>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>COLLECTION (7 criteria) cont.</b>		<b>The entity collects personal information only for the purposes identified in the notice.</b>				
<b>Collection by Fair and Lawful Means (4.2.2)</b>	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.
<b>Collection from Third Parties (4.2.3)</b>	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.
<b>Information Developed About Individuals (4.2.4)</b>	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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>USE, RETENTION AND DISPOSAL (5 criteria)</b>	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.					
<b>Privacy Policies (5.1.0)</b>	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.
<b>Communication to Individuals (5.1.1)</b>	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 to individuals 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.
<b>Use of Personal Information (5.2.1)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>USE, RETENTION AND DISPOSAL (5 criteria) cont.</b>	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.					
<b>Retention of Personal Information (5.2.2)</b>	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.
<b>Disposal, Destruction and Redaction of Personal Information (5.2.3)</b>	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.
<b>ACCESS (8 criteria)</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Privacy Policies (6.1.0)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>		The entity provides individuals with access to their personal information for review and update.				
<b>Communication to Individuals (6.1.1)</b>	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.
<b>Access by Individuals to their Personal Information (6.2.1)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>		The entity provides individuals with access to their personal information for review and update.				
<b>Confirmation of an Individual's Identity (6.2.2)</b>	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.
<b>Understandable Personal Information, Time Frame, and Cost (6.2.3)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>		The entity provides individuals with access to their personal information for review and update.				
<b>Denial of Access (6.2.4)</b>	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.
<b>Updating or Correcting Personal Information (6.2.5)</b>	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		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>ACCESS (8 criteria) cont.</b>	The entity provides individuals with access to their personal information for review and update.					
<b>Statement of Disagreement (6.2.6)</b>	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.
<b>DISCLOSURE TO THIRD PARTIES (7 criteria)</b>	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.					
<b>Privacy Policies (7.1.0)</b>	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.
<b>Communication to Individuals (7.1.1)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>		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.				
<b>Communication to Third Parties (7.1.2)</b>	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.
<b>Disclosure of Personal Information (7.2.1)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>		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.				
<b>Protection of Personal Information (7.2.2)</b>	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.
<b>New Purposes and Uses (7.2.3)</b>	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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>DISCLOSURE TO THIRD PARTIES (7 criteria) cont.</b>		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.				
<b>Misuse of Personal Information by a Third Party (7.2.4)</b>	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.
<b>SECURITY FOR PRIVACY (9 criteria)</b>		The entity protects personal information against unauthorized access (both physical and logical).				
<b>Privacy Policies (8.1.0)</b>	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.
<b>Communication to Individuals (8.1.1)</b>	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
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Information Security Program (8.2.1)</b>	<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 areas<sup>3</sup> insofar as they relate to the security of personal information:</p> <ul style="list-style-type: none"> <li>a. Risk assessment and treatment [1.2.4]</li> <li>b. Security policy [8.1.0]</li> <li>c. Organization of information security [sections 1, 7, and 10]</li> <li>d. Asset management [section 1]</li> <li>e. Human resources security [section 1]</li> <li>f. Physical and environmental security [8.2.3 and 8.2.4]</li> <li>g. Communications and operations management [sections 1, 7, and 10]</li> <li>h. Access control [sections 1, 8.2, and 10]</li> <li>i. Information systems acquisition, development, and maintenance [1.2.6]</li> <li>j. Information security incident management [1.2.7]</li> <li>k. Business continuity management [section 8.2]</li> <li>l. Compliance [sections 1 and 10]</li> </ul>	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.

<sup>3</sup> 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](http://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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Logical Access Controls (8.2.2)</b>	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> <li>a. Authorizing and registering internal personnel and individuals</li> <li>b. Identifying and authenticating internal personnel and individuals</li> <li>c. Making changes and updating access profiles</li> <li>d. Granting privileges and permissions for access to IT infrastructure components and personal information</li> <li>e. Preventing individuals from accessing anything other than their own personal or sensitive information</li> <li>f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities</li> <li>g. Distributing output only to authorized internal personnel</li> <li>h. Restricting logical access to offline storage, backup data, systems and media</li> <li>i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</li> <li>j. Preventing the introduction of viruses, malicious code, and unauthorized software</li> </ul>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Physical Access Controls (8.2.3)</b>	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.
<b>Environmental Safeguards (8.2.4)</b>	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.
<b>Transmitted Personal Information (8.2.5)</b>	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		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>SECURITY FOR PRIVACY (9 criteria) cont.</b>	The entity protects personal information against unauthorized access (both physical and logical).					
<b>Personal Information on Portable Media (8.2.6)</b>	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.
<b>Testing Security Safeguards (8.2.7)</b>	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		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>QUALITY (4 criteria)</b>	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
<b>Privacy Policies (9.1.0)</b>	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.
<b>Communication to Individuals (9.1.1)</b>	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.
<b>Accuracy and Completeness of Personal Information (9.2.1)</b>	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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>QUALITY (4 criteria) cont.</b>	The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.					
<b>Relevance of Personal Information (9.2.2)</b>	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.
<b>MONITORING and ENFORCEMENT (7 criteria)</b>	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
<b>Privacy Policies (10.1.0)</b>	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.
<b>Communication to Individuals (10.1.1)</b>	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		MATURITY LEVELS				
CRITERIA	DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MONITORING and ENFORCEMENT (7 criteria) cont.</b>	The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.					
<b>Inquiry, Complaint and Dispute Process (10.2.1)</b>	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.
<b>Dispute Resolution and Recourse (10.2.2)</b>	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 timeframe 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.
<b>Compliance Review (10.2.3)</b>	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.
<b>Instances of Noncompliance (10.2.4)</b>	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.

GAPP - 73		MATURITY LEVELS				
CRITERIA	CRITERIA DESCRIPTION	AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<b>MONITORING and ENFORCEMENT (7 criteria) cont.</b>		The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes.				
<b>Ongoing Monitoring (10.2.5)</b>	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.







# **APPENDIX B**

**DEPARTMENT OF JUSTICE**

### 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, coordinated all of the work 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 Justice (“Justice”) meets its responsibilities through programs it offers through its divisions of:

- Community Justice & Policing;
- Corporate Services;
- Corrections;
- Court Services;
  - Court Registries,
  - Court Reporters Office,
  - Sheriff’s office.
- Directorate;
- Legal;
- Legal Registries; and
- Policy and Planning.

Justice collects personal information through the divisions listed above as well as its boards and agencies:

- Coroner Service;
- Judicial Remuneration Commission;
- Legal Aid Commission;
- Maintenance Enforcement Program;
- Northwest Territories Review Board;
- Office of the Regulator of Oil and Gas Operations;
- Public Trustee Office;

# DEPARTMENT OF JUSTICE

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

- Rental Office; and
- Victims Assistance Committee.

Personal information collected as part of Coroner Services is governed by the Coroner's Act that includes notwithstanding clauses that result in this Act superseding ATIPP and as such personal information is collected under the Coroner's Act rather than ATIPP. Given that the department works to meet this legislation, rather than specifically ATIPP, the personal information managed under this Act has been excluded from the scope of this report.

Personal information collected as part of Corrections is stored on the APPGEN system, COMS database, FSCC Phone System, Genesis, Inmate Phone System, Lenel – NSCF, March Systems – NSCC, MHS, NSCC Phone System, Pelco – NSCC, SMCC Phone System and SMCC Security System. Personal information collected is also stored on Childview database, Appointments and Revocations Database, CSMNET, MEP Website, CanTax and Computrust.

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

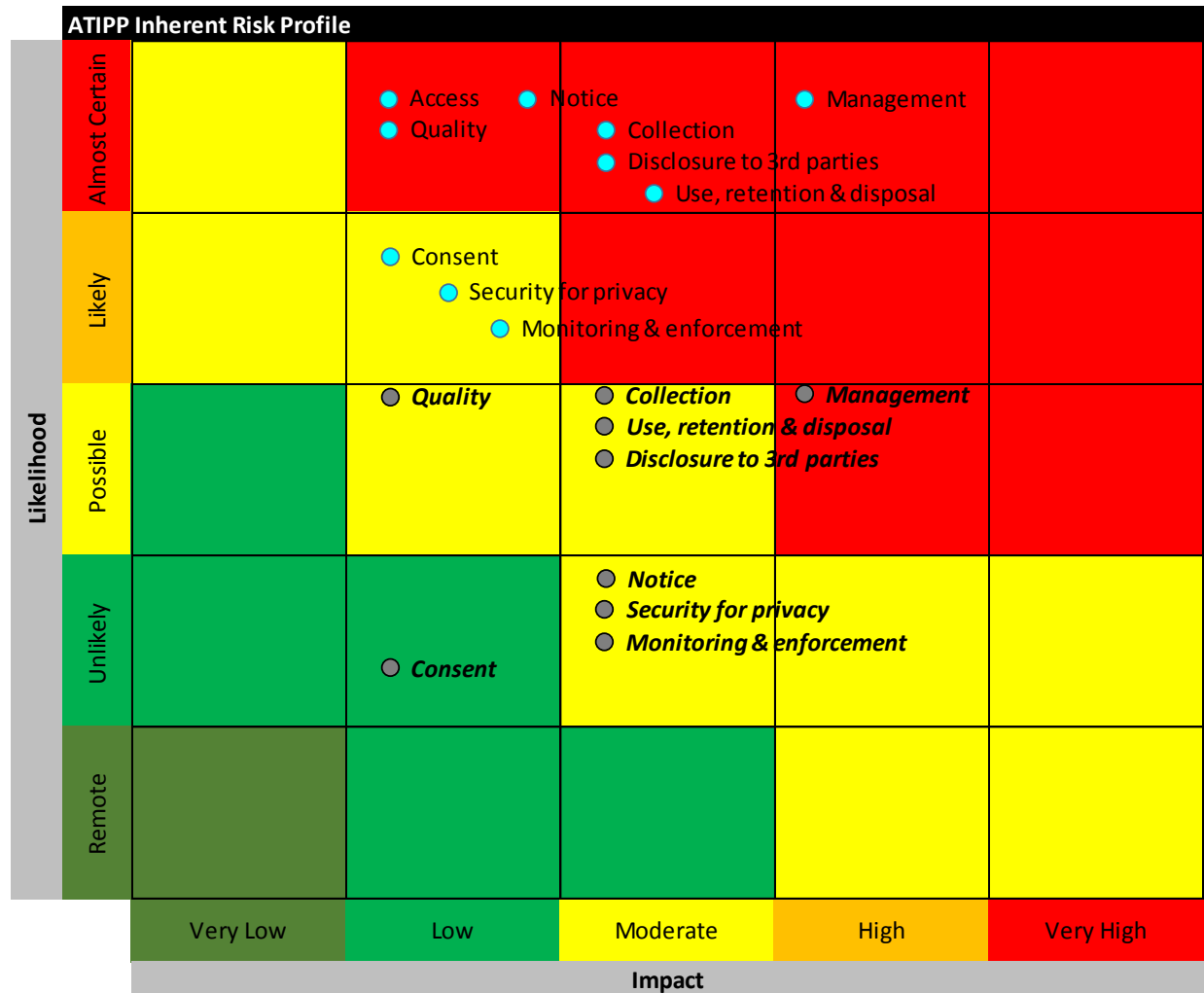
### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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.

# DEPARTMENT OF JUSTICE

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

### RISK HEATMAP



### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

# DEPARTMENT OF JUSTICE

## 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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	N/A	
46	N/A	
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	COMPLIANT	
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	COMPLIANT	
<b>Regulations relating to disclosure of personal information</b>		
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).

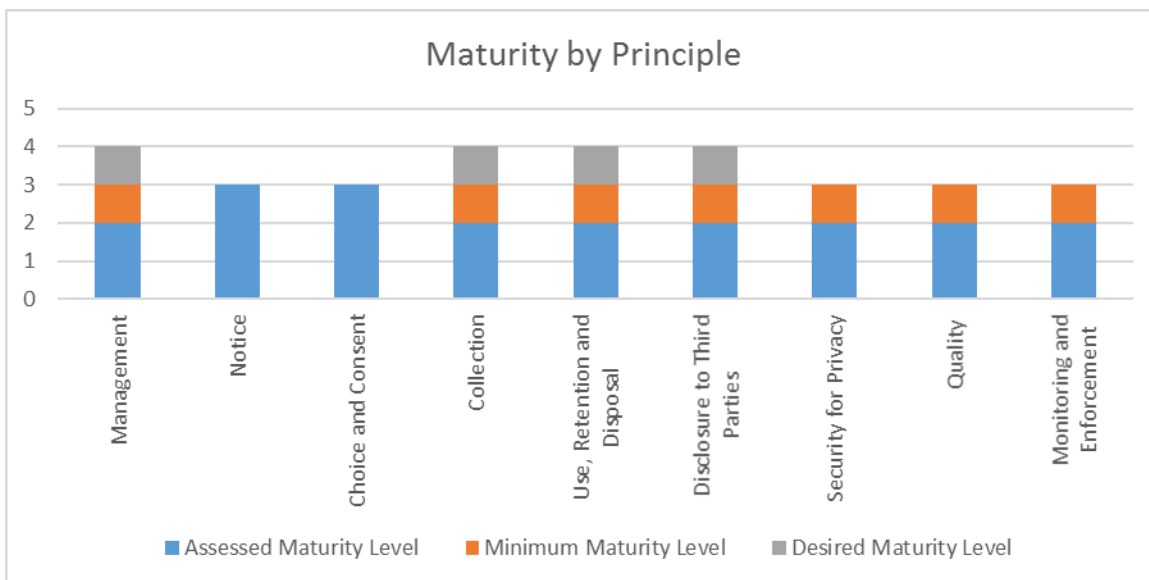
**Desired Maturity Level** – This level would be achieved via long term goals (>24 months) and should be part of long term planning if applicable to your department.

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

# DEPARTMENT OF JUSTICE

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

adequate protection of data. Justice falls into this category, and is therefore expected to plan for the desired maturity level in the future.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP coordinator has been assigned and has taken the training offered by the Privacy Office and Manager of the GNWT Access and Privacy Office.</li> <li>The ATIPP coordinator has delegated authority to the department's senior information privacy analyst to assist with ATIPP requirements.</li> <li>ATIPP delegates review and approve procedures and new collection forms for ATIPP compliance however, reviews of pre-existing forms is not done.</li> <li>Privacy Impact Assessments have started to be used for new programs but have not been done for existing programs.</li> </ul> <p><i>See observations 1-2.</i></p>

# DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<b>Notice</b> The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.	Defined	<ul style="list-style-type: none"><li>• A privacy policy has not been formally designed and documented to address notice to individuals.</li><li>• Notice is provided on forms used to collect personal information.</li></ul> <p><i>See observation 1.</i></p>
<b>Consent</b> 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.	Defined	<ul style="list-style-type: none"><li>• A privacy policy has not been formally designed and documented to address consent of individuals.</li><li>• Implicit consent and explicit consent is obtained on information collection forms when sensitive information is collected.</li></ul> <p><i>See observation 1.</i></p>
<b>Collection</b> The department collects personal information only for the purposes identified in the notice.	Repeatable	<ul style="list-style-type: none"><li>• A privacy policy has not been formally designed and documented to address collection of personal information.</li><li>• The type of personal information collected and the method of collection is known to the individual and the department discloses the collection of information through the use of cookies.</li><li>• Methods and forms of collecting information are provided to the ATIPP coordinator for review before implementation to ensure collection is fair and by lawful means and is limited to that necessary for the purposes identified in the notice.</li></ul> <p><i>See observations 1.</i></p>

# DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>• A formal procedure/process does not exist to ensure information collected is only used for the purpose for which it was collected; review by ATIPP coordinator is done on method of collection to ensure only information needed is collected.</li> <li>• 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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Disclosure to third parties</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Information sharing agreements exist with other departments to provide instructions or requirements 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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of Digital Integrated Information Management System (DIMs) and database restrictions put in place. Physical access to personal information is restricted through various safeguards.</li> </ul>



# DEPARTMENT OF JUSTICE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>Tests of safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></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"> <li>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.</li> <li>Methods of collecting information are provided to the ATIPP coordinator for review before implementation to ensure information collected is relevant for its use.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>Inquiry, complaint and dispute procedures exist but are not formally documented.</li> <li>Monitoring and enforcement are not being done at present.</li> </ul> <p><i>See observation 1.</i></p>

## Observations and Recommendations

### Observation 1

#### Privacy policy has not been designed and documented

- The ATIPP coordinator has limited time and resources to dedicate to ATIPP policies and procedures, specifically in regards to part 2 of the legislation.
- Procedures exist within divisional documents such as the Corrections Service Directives which address relevant privacy principles.

#### 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 who is manager of the office of the GNWT Privacy Office

# DEPARTMENT OF JUSTICE

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

### 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:
The Department of Justice, GNWT Access and Privacy Office has drafted a GNWT Protection of Privacy Policy which has been shared with all departments for review and discussion. It is anticipated that the Policy will be finalized by June 30, 2018.	June 2018
Justice departmental processes and procedures will be set up throughout the Department in order to meet the overarching policy and guidelines.	March 2019
The draft Protection of Privacy Policy is part of an overarching GNWT Privacy Framework that is being developed to support departments in ensuring that the privacy provisions of the ATIPP Act are administered in a consistent and fair manner. The framework will include Privacy Management Program guidelines which are intended to address the overall privacy risks, etc. These guidelines are drafted and are being reviewed by departments.	June 2018

### 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.
- Third parties involved are not identified and documented.

### Risk Profile:

Risk Impact	Without an inventory of personal information, it is not possible for the department to ensure that all areas containing personal information are adequately protected under ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP coordinator who is manager of the office of the GNWT Privacy Office

# DEPARTMENT OF JUSTICE

## 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, 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:
The Department of Justice will compile a listing of personal information collected by each division.	June 2018
It is unclear how third parties are defined in relation to this Audit but once clarified, the Department will include a listing of third parties in relation to the personal information inventory.	June 2018

Responses were provided by Denise Anderson with copies to Mandi Bolstad and Richard Robertson.

# **APPENDIX C**

**DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT**

### 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, coordinated all of the work 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 Education Culture and Employment meets its responsibilities through three branches with the following functions:

- Corporate Services;
- Education and Culture; and
- Labour and Income Security.

Within the functions noted above, divisions and regions collect various types of personal information across multiple programs, which include:

- Early Childhood Development and Learning;
- Labour Development and Standards Division;
- Francophone Affairs Secretariat;
- Teaching and Learning;
- Culture and Heritage;
- Territorial Library Services;
- Education Operations and Development;
- Health, Wellness and Student Support;
- Income Security Programs;
- Student financial Assistance;
- Public Library Services;
- French Translation Services;
- Policy, Legislation and Communications
- Finance and Capital Planning; and
- Planning, Research and Evaluation;

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

The information relation to the programs above are held in a variety of databases. The main electronic system is CMASPR2 (known to staff members as “CMAS”) which holds information relating to Income Assistance, Student Financial Assistance, Employment Development, Education, Operations and Development, Apprenticeship and other programs. Other databases include LIMS, which holds Employment Standards data and IM2SAM which holds departmental finances. There are also various areas which hold personal information in paper files.

Each program, within the department, is responsible for the implementation of its own records classification system. All areas use the Administrative Records Classification System, and some programs have implemented the Operational Records Classification system. Some programs have not adopted any operational records classification system to date.

### Methodology

ECE is a very large department with extremely varied services for which each area has a head who is responsible to some degree for ATIPP Part 2 compliance. As a result it was determined that for this department, interviews would be conducted with the Deputy Minister, ATIPP Coordinator and activity area Director, as well as with the people who were responsible for compliance in each program area. From these interviews it was determined that there were many different approaches to ATIPP Part 2 compliance and level of maturity. In order to obtain a better sense of the differences, two program areas were chosen for a deeper look, Student Financial Assistance, and Educations Operations and Development. The findings for the maturity model portion of the report are determined from the review of these areas as well as per the interviews. Detailed review of forms, etc. was performed at the program review level. It is noted that although overall, the department was rated Ad Hoc in the maturity ratings, there are large variances in understanding of ATIPP Part 2 legislation and in the application of controls – some department areas have much stronger controls in place than others. The overall rating reflects the large variances between program areas.

### Overview

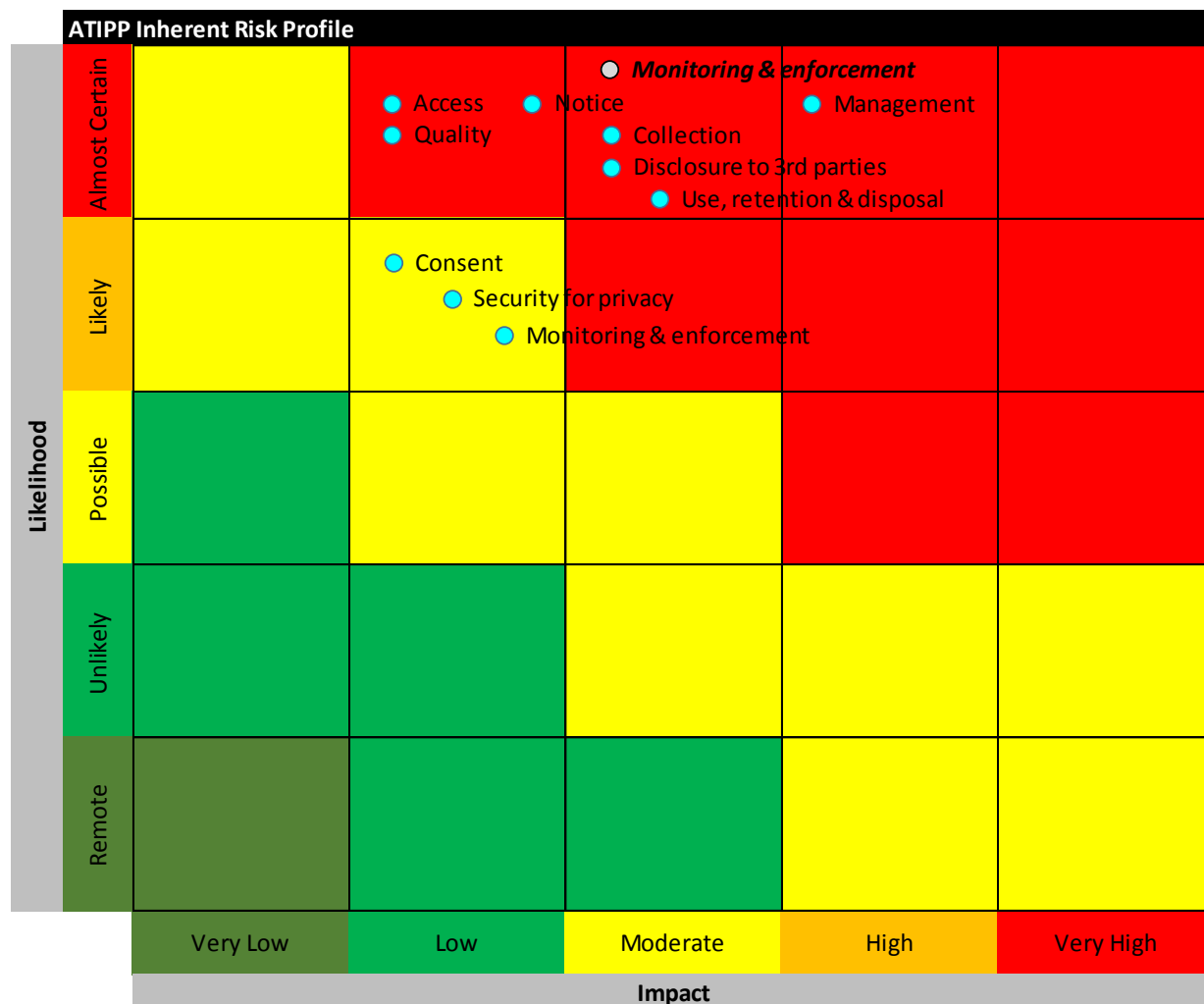
#### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT overall, based on the IAB’s risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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. In the case of ECE it was noted that there are no controls in relation to monitoring and enforcement and that due to the particular nature of the information in this area they felt the likelihood was higher than the overall GNWT rating demonstrated, therefore we have shown an adjusted rating for this principle that is of higher risk. This is denoted in **bold print**.

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### RISK HEATMAP



### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant. There may be areas within a program where partial compliance is in place, but for the purposes of this table, the department has been rated as compliant, non-compliant, or unverifiable.

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		

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

Section	Compliance Assessment	Reason for Non-Compliance
40	NOT COMPLIANT	Per interviews conducted it was determined that there may be information collected outside of the parameters of this section
41 (1)	NOT COMPLIANT	Per program area review, information may be collected from third parties without authorization from the individual. It could not be fully determined that the information was necessary to determine eligibility in a program.
41 (2) & (3)	NOT COMPLIANT	Notice, contact information, and the legal authority for collecting the information is not provided on all forms reviewed as part of the program area review. Principle of collection is not completely met.
42	NOT COMPLIANT	Reasonable security arrangements to protect personal information are not in place in relation to paper files per program area review.
<b>Part 2: Division B – Use of Personal Information</b>		
43	NOT COMPLIANT	Per program area review, information is being used either without consent of the individual and for a different use than for which it was collected.
44	NOT COMPLIANT	Per program area review, processes are not in place to ensure the information is accurate and complete.
45	COMPLIANT	
46	N/A	A disclosure has not been identified.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	UNVERIFIED	A full inventory of personal information has not been completed. Full disclosure cannot therefore be verified.
47.1	UNVERIFIED	No reporting received to date to indicate non-compliance, but unable to confirm full compliance.
48	NOT COMPLIANT	Full disclosure not supported by review of department areas during audit.
49	NOT COMPLIANT	Full disclosure not supported by review of department areas during audit.
<b>Regulations relating to disclosure of personal information</b>		
5	NOT COMPLIANT	Non-compliance under 43 and 48 do not allow for compliance in this area
6	N/A	No formal examination noted.
8	UNVERIFIED	No research agreement in place in areas tested.

### 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).

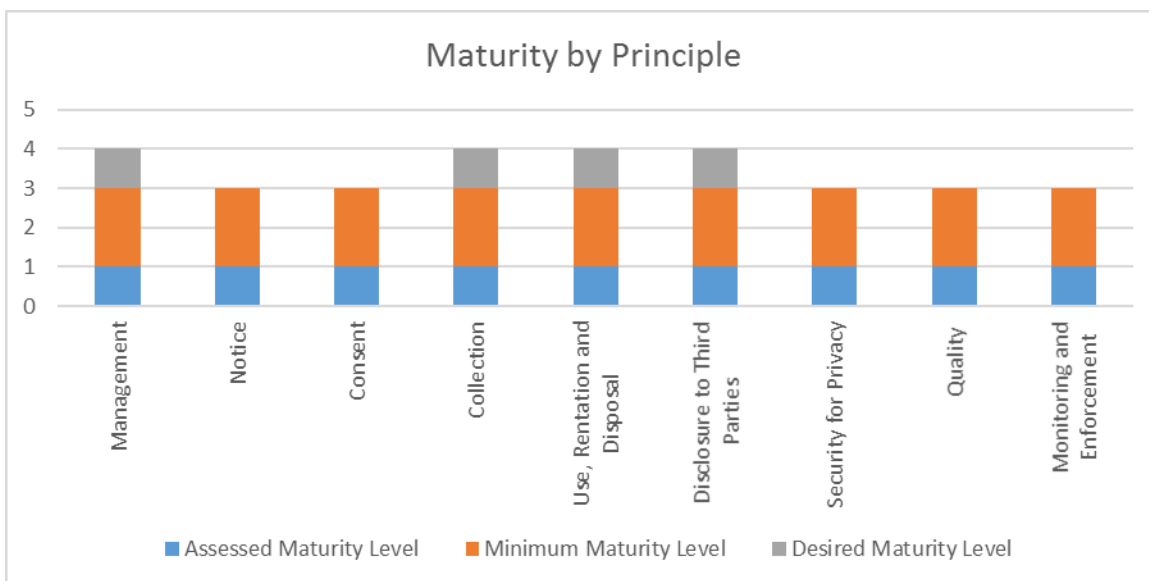


# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

**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. ECE falls into this category, and is therefore expected to plan for the desired maturity level in the future.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>Most of the authority for ATIPP Part 2 compliance has been delegated to program directors (or archivist) and regional superintendents.</li> <li>Privacy policies have not been formally designed and documented.</li> <li>Each program has a different level of understanding of ATIPP Part 2 and the level of accountability required.</li> <li>Privacy policy design has been left to the interpretation of the individual responsible for ATIPP compliance in that program area. These individuals can obtain guidance from the ATIPP coordinator upon request, and can refer to the "ATIPP Policy and Guidelines Manual" produced by Justice.</li> <li>An overall inventory does not exist of the types of personal information and the related processes, systems, and third parties involved,</li> </ul>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>although there are some inventories within program areas.</p> <ul style="list-style-type: none"> <li>An ATIPP Coordinator has been assigned and has taken the training offered by the Privacy Office. The Coordinator has also taken additional privacy training which was supported by the department.</li> <li>The ATIPP Coordinator position is funded for this department and but there remains a lack of resources required for the maturity to be more than Ad Hoc due to the size and complexity of the department.</li> <li>Due to the departmental structure of the role, the ATIPP Coordinator does not have the authority to ensure compliance with the legislation.</li> </ul> <p><i>See observations 1-4.</i></p>
<p><b>Notice</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>There is no consistent privacy policy across the programs; or in some programs no policy that has been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms (hard copy and online) used to collect personal information.</li> </ul> <p><i>See observation 5.</i></p>
<p><b>Consent</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>There is no consistent privacy policy across the programs; or in some programs no policy that has been formally designed and documented to address notice to individuals.</li> <li>Implicit and explicit consent is not consistently obtained before the collection of information across the programs.</li> </ul> <p><i>See observation 6.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>There is no consistent privacy policy across the programs; or in some programs no policy that has been formally designed and documented to address notice to individuals.</li> <li>Methods and forms of collecting information are not required to be provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means. The Coordinator does review some new forms but only on a basis of request, rather than requirement.</li> <li>Although the Coordinator does follow guidelines from the “ATIPP Policy and Guidelines Manual”, a required procedure/process does not exist to ensure only information needed is collected and to ensure authorization takes</li> </ul>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>place if information is not collected directly from the individual under 41(1).</p> <p><i>See observations 8-9.</i></p>
<p><b>Use, retention and disposal</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>• There is no consistent privacy policy across the programs; or in some programs no policy that has been formally designed and documented to address notice to individuals.</li> <li>• A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for and to ensure disclosure takes place to the individual if the use of the information changes.</li> <li>• Each program is responsible for the implementation of its own records classification system. All programs have implemented the Administrative Records Classification System, and some programs have implemented the Operational Records Classification systems, Some programs have not adopted any operational records classification system to date.</li> </ul> <p><i>See observation 9.</i></p>
<p><b>Disclosure to third parties</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>• There is no consistent privacy policy across the programs; or in some programs no policy that has 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.</li> <li>• Information sharing agreements do not consistently exist with other departments to provide instructions or requirements 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.</li> <li>• Information sharing agreements are not consistently in place across the programs for third parties.</li> </ul> <p><i>See observation 10.</i></p>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• There is no consistent privacy policy across the programs; or in some programs no policy that has been designed and documented to address security for privacy.</li> <li>• Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>• Personal devices are being used to transmit data.</li> <li>• Tests of safeguards in place are not performed.</li> </ul> <p><i>See observation 11.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• There is no consistent privacy policy across the programs; or in some programs no policy that has been designed and implemented 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.</li> <li>• There are no consistent processes in place across the department to ensure that information entered into documents is accurate</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></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"> <li>• There is no consistent privacy policy across the programs; or in some programs no policy that has been designed and documented to address monitoring and enforcement.</li> <li>• Monitoring and enforcement are not being done at present.</li> </ul> <p><i>See observation 1.</i></p>

### Observations and Recommendations

#### Observation 1

##### Privacy policy has not been designed and documented

- The responsibility and authority to develop the privacy policies has been unclear.
- The ATIPP Coordinator has limited time and resources to dedicate to ATIPP policies and procedures, specifically in regards to part 2 of the legislation.

#### 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 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:
ECE will work with the Department of Justice to develop and implement an ECE Privacy Management Program once the policy and associated guidelines for such a program have been established by the Department of Justice. If it is the expectation of the Department of Justice that Departments meet the minimum privacy maturity model principles, then this expectation should be outlined in the policy and associated guidelines.	Within one year of the policy and guidelines being finalized by the Department of Justice.

#### Observation 2

##### ATIPP Part 2 compliance has been delegated to the program level

- ATIPP Part 2 compliance has been delegated to individuals within each program area with limited guidance. Advice is provided by the Coordinator when requested but limited resourcing results in limits in this individual's capacity to do so.
- These individuals have been left to interpret ATIPP and create their own policies and/or procedures, if at all, with no implementation timeline established and maintained.
- These individuals have different levels of understanding of ATIPP.

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Risk Profile:

Risk Impact	Delegation of ATIPP compliance requirements to individual division heads has left those without a complete understanding of the legislation in charge of ensuring compliance. This results in non-compliance with the ATIPP legislation.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

### Recommendations:

We recommend that:

- Authority for ensuring compliance with ATIPP should be kept at the department level and not delegated down to program areas. Process development to meet departmental requirements for ATIPP can remain at the program level, but overall requirements should be set at the department level.
- ATIPP training should be required by all individuals with any responsibility for compliance or those whose processes include steps required for compliance. This will ensure that processes developed and followed by program areas to meet departmental requirements will be adequate.

### Management Response:

Action Plan	Completion Date:
ECE will review the authorities for compliance as part of the development of the ECE Privacy Management Program	<ul style="list-style-type: none"> <li>• ECE Privacy Management Program will be developed and implemented within one year of the policy and guidelines being finalized by the Department of Justice.</li> <li>• Training and implementation of the ECE Privacy Management Program will be ongoing.</li> </ul>
The Access to Information and Protection of Privacy General Awareness on-line training will be made mandatory for all ECE staff as part of their 2018-2019 performance objectives	March 31, 2019 and ongoing as new staff are employed within ECE.
Provide general awareness privacy training and a briefing on the delegation of authority responsibilities for senior managers to ECE's Executive Committee	Training / briefing session to be provided at one of the Executive Committee meetings held between April – June of each fiscal year
Privacy training provided as part of the program-based privacy audits referenced in the actions related to observations 5-11	As per the program-level audit schedule

### Observation 3

#### An inventory of personal information collected does not exist

- Individuals from program areas who are responsible for ATIPP Part 2 compliance are responsible for inventorying personal information collected.
- These individuals have different understandings of what personal information is and how it should be inventoried.
- There is no consistent system or method used across the programs for tracking personal information collected.
- Some programs are not fully aware of how much personal information they have or where it is located.
- Systems involved in collection and storage of personnel information are not documented.
- Third parties are not consistently identified and 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 adequately protected under ATIPP.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

#### 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 program area 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.
- A consolidated areas of responsibility document is developed outlining the personal information being collected by each program and who is to ensure compliance.

#### Management Response:

Action Plan	Completion Date:
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>- related processes including:                             <ul style="list-style-type: none"> <li>o forms, and their revision dates,</li> <li>o systems and other data banks, and related security arrangements</li> <li>o storage locations of hard copies, and existing security arrangements,</li> </ul> </li> </ul>	<p>September 30, 2018 to complete the initial inventory and then annual reviews thereafter.</p>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

<ul style="list-style-type: none"> <li>○ third parties involved (including information sharing agreements), and</li> <li>○ staff responsibility for ensuring compliance.</li> </ul>	
---	--

### Observation 4

**The department resources are inadequate to address the volume of work require for compliance with ATIPP Part 2 and Coordinator does not have authority to ensure compliance.**

- The current resource capacity is inadequate to address the full compliance requirements of ATIPP Part 2.
- The role of ATIPP Coordinator is situated within the department in a position without the authority to ensure that there is departmental compliance with ATIPP Part 2. The Coordinator therefore acts in an advisory role only.

### Risk Profile:

Risk Impact	<p>ATIPP requests may go unaddressed with or exceed the timelines set out in the ATIPP legislation to address requests.</p> <p>Without the Coordinator role having the authority to ensure compliance, there is increased risk that ATIPP Part 2 legislation will not be met.</p>
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

### Recommendations:

We recommend that:

- A review of resourcing be performed to determine what would be required to meet the full compliance requirements of the ATIPP Part 2 legislation.
- A review of the placement and reporting of the ATIPP Coordinator role be performed. It is recommended that the department consider placing this role in a position where reporting up to the DM is possible. This would provide the authority needed in the role to ensure departmental compliance.

### Management Response:

Action Plan	Completion Date:
ECE will review the resourcing requirements, placement and reporting of the privacy function with the goal of ensuring departmental compliance to ATIPP Part 2	July 31, 2018



# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Observation 5

#### Forms, hard copy and electronic, used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from most forms reviewed during the program area review.
- The department is not fully compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.

#### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

#### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to provide the required notice to the individuals.

#### Management Response:

Action Plan	Completion Date:
ECE will create and maintain an inventory of personal information that will identify: <ul style="list-style-type: none"><li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li><li>- related processes including:<ul style="list-style-type: none"><li>o forms, and their revision dates,</li><li>o systems and other data banks, and related security arrangements</li><li>o storage locations of hard copies, and existing security arrangements,</li><li>o third parties involved (including information sharing agreements), and</li><li>o staff responsibility for ensuring compliance.</li></ul></li></ul>	September 30, 2018 to complete the initial inventory and then annual reviews thereafter.
ECE will develop and implement a schedule for conducting a program-based privacy audit based	Schedule to be developed by March 31, 2019 with implementation as per the schedule

<p>on the inventory of personal information. The schedule would be prioritized through a risk-based assessment and take current ATIPP resources into consideration. The purpose of the program privacy audit will be to review collection methods in relation to compliance with the Act Part 2 and best practices, including confirmation that the information is necessary, and includes appropriate notices to the individual regarding collection, use and disclosure. The audit process will also identify the need for, the following:</p> <ul style="list-style-type: none"> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li> <li>- improving physical security for hard copy records containing personal information.</li> </ul>	
---	--

### Observation 6

#### Not all forms, hard copy and electronic, used to collect personal information require consent from the individual

- Implicit consent is obtained by the individual’s signature on the collection form but not all forms require the signature of the individual.
- Explicit consent is not obtained when sensitive information is collected. Although this is not a requirement of ATIPP legislation, it is considered best practice.

#### Risk Profile:

Risk Impact	When consent is not obtained there is an increased risk that full disclosure to the individual as the use of that information has not been made; which would result in non-compliance with ATIPP
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to require the individual's signature or explicit consent if sensitive information is being collected.

### Management Response:

Action Plan	Completion Date:
As the ATIPP Act currently does not require consent, ECE will consider this recommendation as part of its action to update forms outlined in observation 5.	Based on the schedule to be implemented as an action through Observation 5.

### Observation 7

#### Methods of collection are not consistently reviewed by ATIPP Coordinator prior to implementation

- Department develops and uses their own methods of collection of personal information.
- New collection methods are therefore not always reviewed by ATIPP Coordinator along with key stakeholders as required to ensure they are fair and lawful. As these are not required to be reviewed, the Coordinator will only see the methods that the department choose to bring forward for review.
- New collection methods are not consistently reviewed to ensure only information needed for its purpose is being collected. A privacy impact assessment is not always performed when needed.

### Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

### Recommendations:

We recommend that:

- A procedure be formalized that requires all new methods of information collection be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized which specifies actions to be taken by the ATIPP Coordinator to validate only information needed is collected through fair and lawful means.
- A privacy impact assessment be performed for all new information collection methods or changes to existing methods.

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Management Response:

Action Plan	Completion Date:
ECE will develop and communicate to ECE Senior Managers a procedural flow chart to indicate when reviews are required or the ATIPP Coordinator should be consulted for all new and / or revised methods of information collection.	Procedural flow chart developed and communicated by June 30, 2018
ECE will develop, promote and implement a Privacy Management Program which will formalized approval processes for all new and / or revised methods of information collection.	<ul style="list-style-type: none"> <li>ECE Privacy Management Program will be developed and implemented within one year of the policy and guidelines being finalized by the Department of Justice.</li> <li>Promotion and implementation of the ECE Privacy Management Program will be ongoing.</li> </ul>
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>related processes including:                             <ul style="list-style-type: none"> <li>forms, and their revision dates,</li> <li>systems and other data banks, and related security arrangements</li> <li>storage locations of hard copies, and existing security arrangements,</li> <li>third parties involved (including information sharing agreements), and</li> <li>staff responsibility for ensuring compliance.</li> </ul> </li> </ul>	September 30, 2018 to complete the initial inventory and then annual reviews thereafter.
ECE will develop and implement a schedule for conducting a program-based privacy audit based on the inventory of personal information The schedule would be prioritized through a risk-based assessment and take current ATIPP resources into consideration. The purpose of the program privacy audit will be to review collection methods in relation to compliance with the Act Part 2 and best practices, including confirmation that the	Schedule to be developed by March 31, 2019 with implementation as per the schedule

<p>information is necessary, and includes appropriate notices to the individual regarding collection, use and disclosure. The audit process will also identify the need for, the following:</p> <ul style="list-style-type: none"> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li> <li>- improving physical security for hard copy records containing personal information.</li> </ul>	
--	--

### Observation 8

#### Procedures do not exist to ensure only information needed is collected

- Existing methods of collection are not required to be reviewed by ATIPP Coordinator along with key stakeholders as required to ensure only information needed is being collected.

#### Risk Profile:

Risk Impact	If additional information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

#### Recommendations:

We recommend that:

- The department reevaluate and reassess the current information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Management Response:

Action Plan	Completion Date:
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>- related processes including:                             <ul style="list-style-type: none"> <li>o forms, and their revision dates,</li> <li>o systems and other data banks, and related security arrangements</li> <li>o storage locations of hard copies, and existing security arrangements,</li> <li>o third parties involved (including information sharing agreements), and</li> <li>o staff responsibility for ensuring compliance.</li> </ul> </li> </ul>	<p>September 30, 2018 to complete the initial inventory and then annual reviews thereafter.</p>
<p>ECE will develop and implement a schedule for conducting a program-based privacy audit based on the inventory of personal information. The schedule would be prioritized through a risk-based assessment and take current ATIPP resources into consideration. The purpose of the program privacy audit will be to review collection methods in relation to compliance with the Act Part 2 and best practices, including confirmation that the information is necessary, and includes appropriate notices to the individual regarding collection, use and disclosure. The audit process will also identify the need for, the following:</p> <ul style="list-style-type: none"> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT</li> </ul>	<p>Schedule to be developed by March 31, 2019 with implementation as per the schedule</p>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

<p>departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</p> <ul style="list-style-type: none"> <li>- improving physical security for hard copy records containing personal information.</li> </ul>	
--	--

### Observation 9

#### Indirect collection of data may not be correctly authorized

- A process is not in place to ensure that authorization is obtained from the individual to whom the information pertains when personal information is collected indirectly and the collection does not fall under the exceptions noted in 41(b-j).

#### Risk Profile:

Risk Impact	When collection of personal information is not authorized by the individual to whom it relates, the department may not be in compliance with ATIPP Part 2 legislation
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

#### Recommendations:

We recommend that:

- Privacy procedures be developed to address situations and/or circumstances where personal information is developed or acquired about individuals, and a process be implemented to ensure individuals are informed and that authorization is obtained when required.

#### Management Response:

Action Plan	Completion Date:
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>- related processes including:                             <ul style="list-style-type: none"> <li>o forms, and their revision dates,</li> <li>o systems and other data banks, and related security arrangements</li> <li>o storage locations of hard copies, and existing security arrangements,</li> </ul> </li> </ul>	<p>September 30, 2018 to complete the initial inventory and then annual reviews thereafter.</p>

<ul style="list-style-type: none"> <li>○ third parties involved (including information sharing agreements), and</li> <li>○ staff responsibility for ensuring compliance.</li> </ul>	
<p>ECE will develop and implement a schedule for conducting a program-based privacy audit based on the inventory of personal information. The schedule would be prioritized through a risk-based assessment and take current ATIPP resources into consideration. The purpose of the program privacy audit will be to review collection methods in relation to compliance with the Act Part 2 and best practices, including confirmation that the information is necessary, and includes appropriate notices to the individual regarding collection, use and disclosure. The audit process will also identify the need for, the following:</p> <ul style="list-style-type: none"> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li> <li>- improving physical security for hard copy records containing personal information.</li> </ul>	<p>Schedule to be developed by March 31, 2019 with implementation as per the schedule</p>

**Observation 10**

**Information sharing agreements do not always exist between departments and third parties**

- A listing does not exist which fully details the type of information shared through information sharing agreements, with which departments and for what use. The existing listing for ECE lists the third party but not the details of type of information and use.
- Information sharing agreements are not consistently in place for all third parties other than GNWT departments.



# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

### Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

### Recommendations:

We recommend that:

- A listing of all information provided to other departments and other third parties be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into, or reviewed and updated as needed, with departments and other third parties that receive necessary personal information from Education Culture and Employment and that the agreements provide instructions or requirements 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.

### Management Response:

Action Plan	Completion Date:
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>- related processes including:                             <ul style="list-style-type: none"> <li>o forms, and their revision dates,</li> <li>o systems and other data banks, and related security arrangements</li> <li>o storage locations of hard copies, and existing security arrangements,</li> <li>o third parties involved (including information sharing agreements), and</li> <li>o staff responsibility for ensuring compliance.</li> </ul> </li> </ul>	<p>September 30, 2018 to complete the initial inventory and then annual reviews thereafter.</p>
<p>ECE will develop and implement a schedule for conducting a program-based audit based on the inventory of personal information. The schedule would be prioritized through a risk-based assessment and take current ATIPP resources</p>	<p>Schedule to be developed by March 31, 2019 with implementation as per the schedule</p>

<p>into consideration. The purpose of the program privacy audit will be to review collection methods in relation to compliance with the Act Part 2 and best practices, including confirmation that the information is necessary, and includes appropriate notices to the individual regarding collection, use and disclosure. The audit process will also identify the need for, the following:</p> <ul style="list-style-type: none"> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li> <li>- improving physical security for hard copy records containing personal information.</li> </ul>	
--	--

### Observation 11

#### Physical security does not exist for all hard copy records of personal information

- Physical access restrictions do not exist for all hard copy records.
- Not all hard copy records containing personal information are stored in secure and locked cabinets per program review.

#### Risk Profile:

Risk Impact	When records are left in locations that can be accessed there is increased risk that personal information will be seen by people who are not part of the use for which the disclosure was made upon collection. This would result in non-compliance with ATIPP legislation.
Risk Responsibility	Assistance Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Privacy Office

#### Recommendations:

We recommend that:

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

- A procedure, as supported by policy, be formalized that details how physical records containing personal information be stored to ensure all documents are stored in secure cabinets with restricted access.
- Storage cabinets or other storage equipment be acquired to allow for restricted access and to prevent accidental disclosure due to natural disasters and environmental hazards.

### Management Response:

Action Plan	Completion Date:
<p>ECE will create and maintain an inventory of personal information that will identify:</p> <ul style="list-style-type: none"> <li>- the types of direct and indirect information that is being collected, for what purpose and by whom; and the</li> <li>- related processes including:                             <ul style="list-style-type: none"> <li>o forms, and their revision dates,</li> <li>o systems and other data banks, and related security arrangements</li> <li>o storage locations of hard copies, and existing security arrangements,</li> <li>o third parties involved (including purpose and use of information and whether the information is required to be shared), and</li> <li>o staff responsibility for ensuring compliance.</li> </ul> </li> <li>- updated forms, both hard copy and electronic so that the required notice to individuals is provided;</li> <li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li> <li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li> <li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li> <li>- improving physical security for hard copy records containing personal information. updated forms, both hard copy and</li> </ul>	<p>Schedule to be developed by March 31, 2019 with implementation as per the schedule</p>

# DEPARTMENT OF EDUCATION CULTURE AND EMPLOYMENT

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

<p>electronic so that the required notice to individuals is provided;</p> <ul style="list-style-type: none"><li>- updated procedures for collection of personal information to be reviewed and approved by the ATIPP Coordinator;</li><li>- privacy impact assessments performed for all new information collection methods or changes to existing methods;</li><li>- developing or updating information sharing agreements with other GNWT departments and its agencies, as well as Third Parties for the purpose of assuring the information shared is required to be shared and that the appropriate instructions for use and protections are included; and</li><li>- improving physical security for hard copy records containing personal information.</li></ul>	
---	--

Responses provided by Jennifer Young with copies to Lorna Dosso, Olin Lovely, Helen Whitworth, Alison Washburn and Sylvia Haener.

# **APPENDIX D**

**DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS**

### 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, coordinated all of the work 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 Executive and Indigenous Affairs (“EIA”) meets its responsibilities through programs it offers through its divisions of:

- Aboriginal Consultation and Aboriginal Relations;
- Cabinet Communications and Protocol;
- Cabinet Secretariat;
- Corporate Communications;
- Directorate;
- Executive Council Offices;
- Implementation;
- Intergovernmental Relations;
- Legislation and House Planning;
- Negotiations;
- Policy, Planning and Communications;
- Priorities and Planning;
- Regional Operations;
- Secretary to Cabinet; and
- Women’s Advisory.

EIA’s collection of personal information is limited to its administration of expression of interest (“EI”) submissions for board appointments. EIA provides the information to the appropriate board or selection committee which is the intended recipient and as such EIA does not provide personal information to third parties.

The EI documents are managed in house and stored on a candidate database.

# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

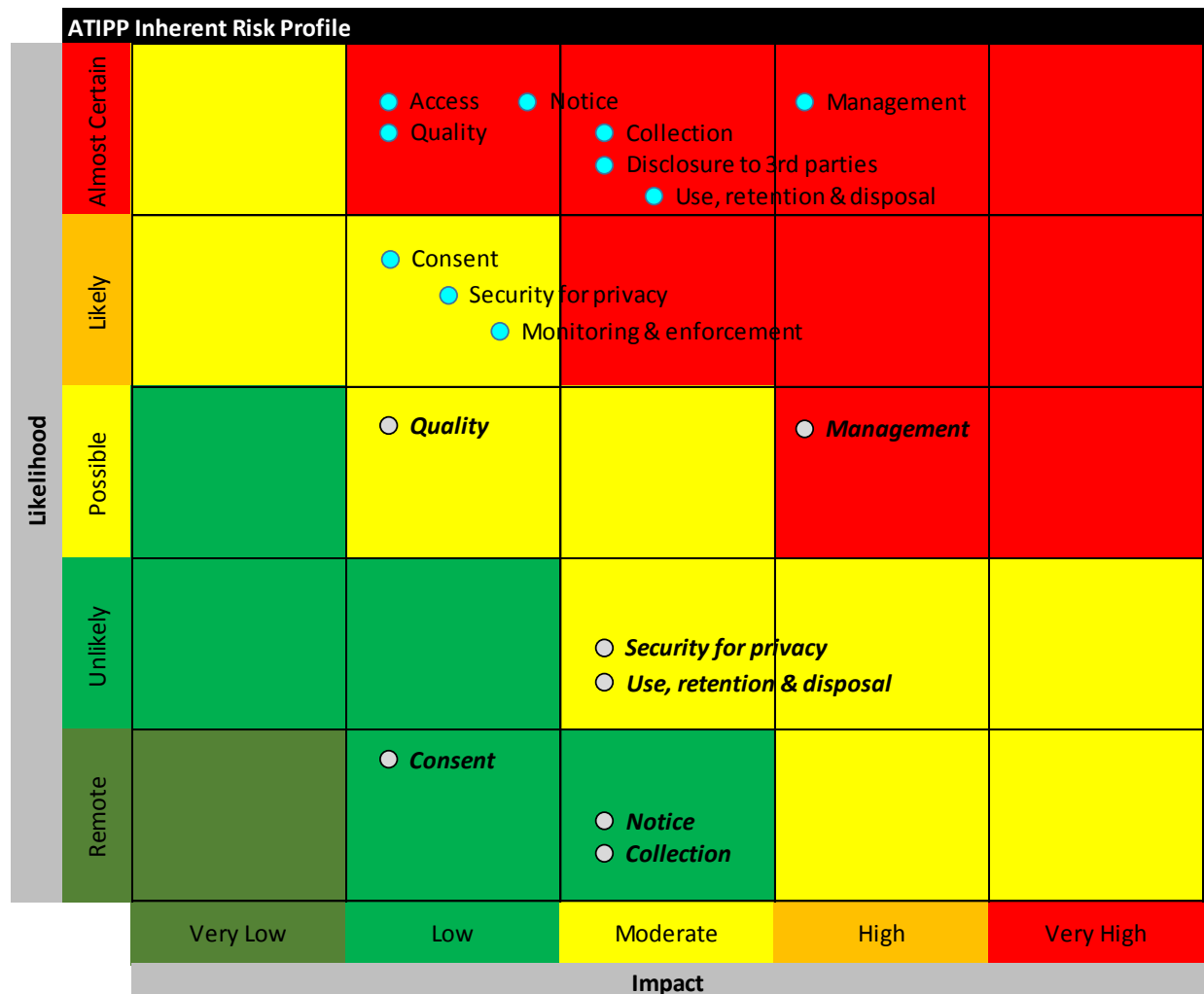
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) PART 2

### Overview

### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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



# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

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

### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	N/A	
46	N/A	
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	N/A	Information is not disclosed.
47.1	N/A	Information is not disclosed.
48	N/A	Information is not disclosed.
49	N/A	Information is not disclosed.
<b>Regulations relating to disclosure of personal information</b>		
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).

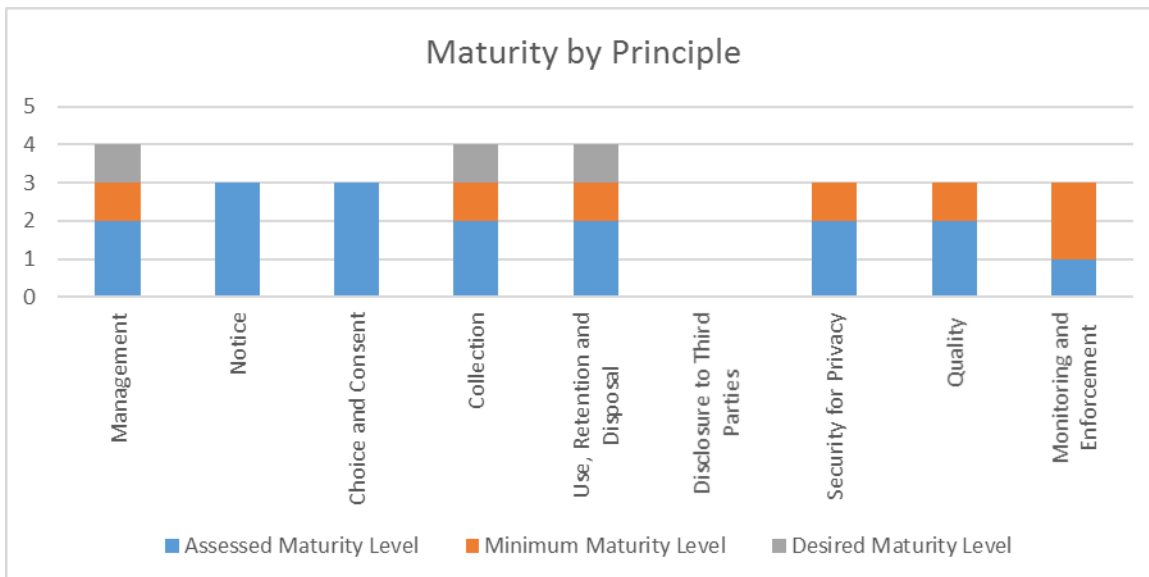


# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

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

**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.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As EIA does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>ATIPP Coordinator duties has been assigned; this individual has taken extensive privacy training and has been involved with privacy training for GWNT in the past.</li> <li>Privacy impact assessments are not used as there are few processes that involve personal information and those that do are very simple.</li> </ul> <p><i>See observations 1-2.</i></p>
<p><b>Notice</b></p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which</p>	Defined	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is provided on forms used to collect personal information.</li> </ul>

# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
personal information is collected, used, retained and disclosed		<i>See observation 1.</i>
<p><b>Consent</b></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>	Defined	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>• Implicit consent and explicit consent is obtained on information collection forms when sensitive information is collected.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>• The type of personal information collected and the method of collection is known to the individual and the department discloses the collection of information through the use of cookies and that information could be acquired.</li> <li>• There are informal and undocumented procedures to ensure collection of information is limited to that necessary for its purpose.</li> <li>• The form used to collect candidate information was developed by the ATIPP Coordinator with privacy requirements taken into consideration.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>• Although a procedures/process has not been documented to ensure information collected is only used for the purpose for which is was collected, as EI forms are the one significant type of personal information collected by the department, and these forms have been designed to collect data for one use, there is less chance of data being used for a different purpose than intended.</li> <li>• A procedure/process has not been documented to ensure information collected is only used for the purpose for which is was collected.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Disclosure to third parties</b></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>	NA	Information is not provided to third parties

# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>Logical access to personal information is restricted by the department through the of the candidate database to store the EIs. Access to the database is limited to those who are involved the board processes. Information is therefore only available to those using it for the use for which is was collected.</li> <li>Security measures exist over the transmission of data per office of the but are not formally designed and documented.</li> <li>Tests of safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></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"> <li>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.</li> <li>The form used for collecting applicant data was developed by the ATIPP Coordinator and designed to collect information relevant to its use.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></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"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>Monitoring and enforcement are not being done at present.</li> </ul> <p><i>See observation 1.</i></p>

## Observations and Recommendations

### Observation 1

#### Privacy policy has not been designed and documented

- The personal information collected by the department is very limited.
- A privacy policy has not been documented for the department.

# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

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

### 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 and of 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:
EIA will be happy to work with DOJ to develop a GNWT-wide policy	To be determined by DOJ

### Observation 2

#### An inventory of personal information collected does not exist

- The personal information collected by the department is very limited but personal information is collected by the department.
- Systems involved in collection and storage of personnel information 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 containing personal information are adequately protected under ATIPP.
Risk Responsibility	Assistant Deputy Minister Priorities and Planning
Risk Mitigation Support	Delegated ATIPP Coordinator and office of the GNWT Access and Privacy Office

# DEPARTMENT OF EXECUTIVE AND INDIGENOUS AFFAIRS

## 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 and 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:
A recommendation will be made that EIA stop the practice of accepting expression of interest on the board's website. The public demand for this service falls far below original expectations and other options are available to interested parties. After this information is disposed of there will be no other personal information held by EIA and therefore no need for an inventory.	N/A

Responses were provided by Alan Cash.

# **APPENDIX E**

**DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES**

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

## 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, coordinated all of the work 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 Environment and Natural Resources (“ENR”) meets its responsibilities through programs it offers through its divisions of:

- Environment;
- Wildlife;
- Water Resources;
- Forest Management; and
- Conservation, Assessment & Monitoring.

ENR collects personal information through:

- Compliance Management Information System – CMIS database;
- Water Quality Monitoring system – Lodestar database;
- Wildfire financial management system – EMBER database;
- Payroll Management for temporary fire operations staff – Easy Pay system;
- Licensing Information system – LISIN database; and
- Fur Harvest Promissory Note Management system – FurHarvest database.

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

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

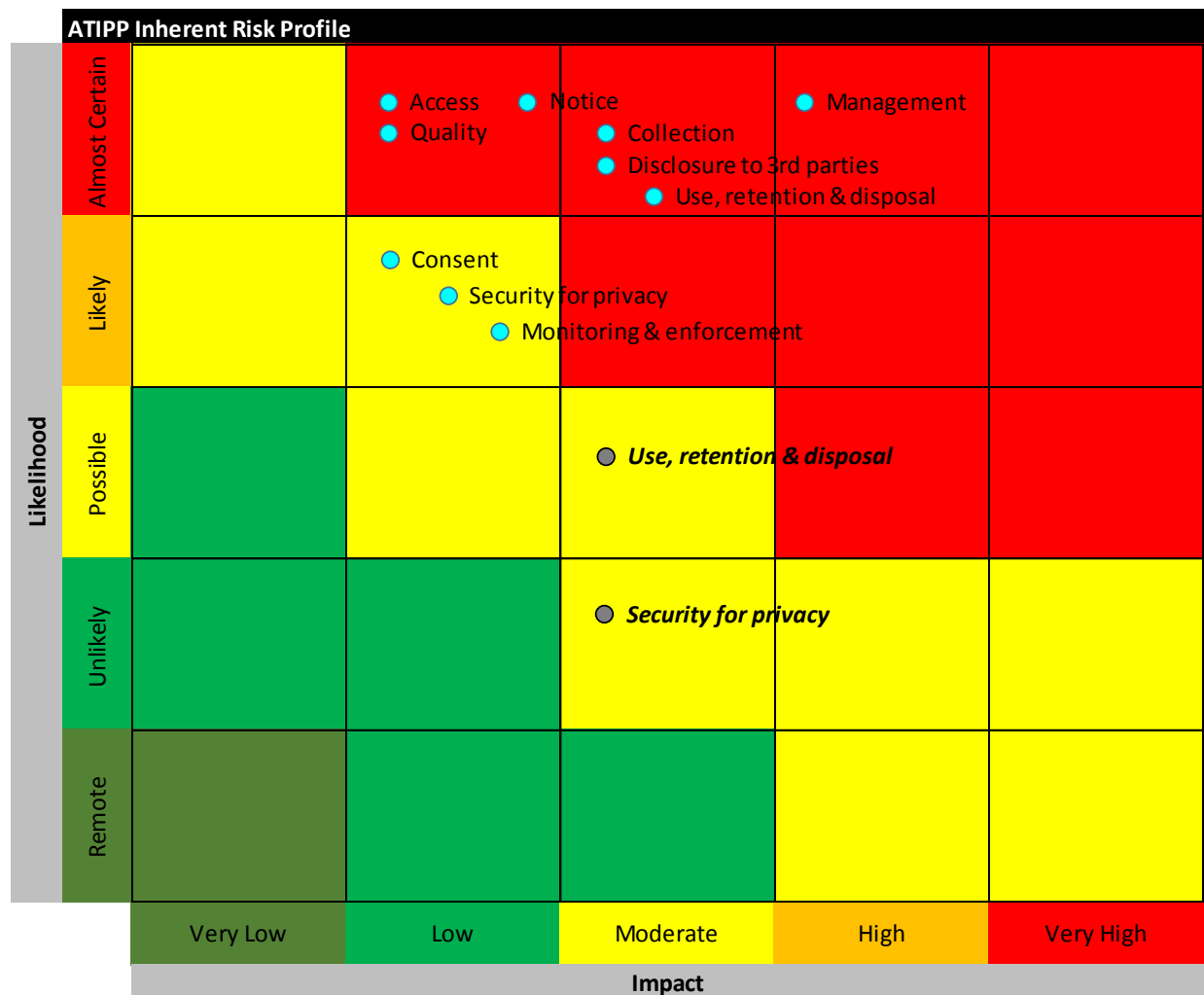
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) PART 2

### Overview

#### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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





# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	NOT COMPLIANT	Legal authority for collection of information and contact information is not provided on all forms. Principle of notice is not completely met.
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
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.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
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 could not be verified.
49	N/A	Information not provided for statistical purposes
<b>Regulations relating to disclosure of personal information</b>		
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.

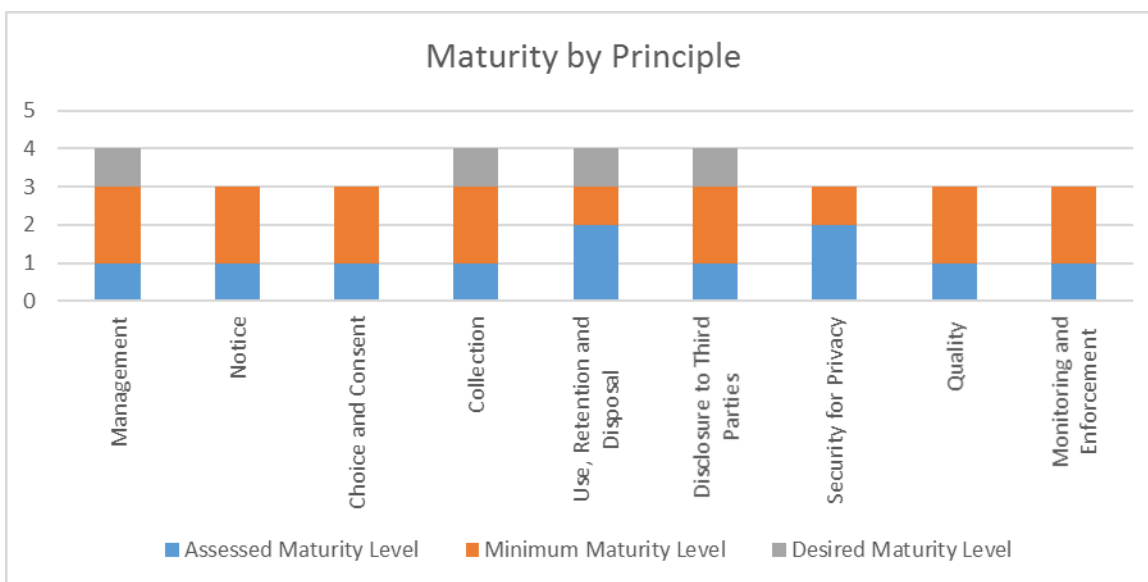
# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

**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.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As ENR does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures</p>	Ad Hoc	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP Coordinator has been assigned and has taken the necessary training offered by the Privacy Office.</li> <li>PIAs have been used.</li> </ul> <p><i>See observations 1-2.</i></p>

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Notice</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms used to collect personal information.</li> </ul> <p><i>See observation 3.</i></p>
<p><b>Consent</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent is obtained on personal information collection forms.</li> <li>Explicit consent is obtained on information collection forms.</li> <li>Consent is not documented when information is collected verbally.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>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.</li> <li>Notice of collection is not documented when information is collected verbally.</li> <li>Methods and forms of collecting information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.</li> <li>A formal procedure/process does not exist to ensure only information needed is collected.</li> </ul> <p><i>See observation 4.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for.</li> <li>Retention and disposal of information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and</li> </ul>

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>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> <p><i>See observation 5.</i></p>
<p><b>Disclosure to third parties</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Information sharing agreements do not exist with other departments to provide instructions or requirements 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.</li> </ul> <p><i>See observation 6.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Shared Services Centre.</li> <li>• Physical access to personal information is restricted through access to building, floor restriction access, storage in secure and locked cabinets.</li> <li>• Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>• Tests of all safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• 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</li> </ul>

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
information for the purposes identified in the notice.		is relevant to the purposes for which it is to be used.  <i>See observation 1.</i>
<b>Monitoring and enforcement</b> The department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>Monitoring and enforcement are not being done at present.</li> </ul> <i>See observation 1.</i>

## Observations and Recommendations

### Observation 1

#### Privacy policy has not been designed and documented

- Some procedures have been used to address privacy matters.
- There is not a fully documented privacy policy in place.

#### 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.

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Management Response:

Action Plan	Completion Date:
ENR will provide input to and then comply with a GNWT-wide privacy policy as developed by Dept. of Justice who oversees the Access to Information and Protection of Privacy Act.	Completion date is the responsibility of the Dept. of Justice.

### 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

### 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:
ENR Communications is in the beginning stages of a form renewal for the department. Through this process, ENR Corporate Services will request inventories of the types of personal information and related processes/systems/third parties involved to be submitted by all divisions to the ATIPP Coordinator for consolidation into a global department inventory. A review will take place to ensure compliance processes and procedures are in place.	March 2019

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Observation 3

#### Forms used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from forms.
- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to legal authority identification and individuals being informed about how to contact the entity with inquiries, complaints and disputes.

#### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- All forms used to collect personal information be reviewed and updated to consistently provide the required notice to the individuals.

#### Management Response:

Action Plan	Completion Date:
ENR Corporate Services will review all forms to collect personal information and update them to consistently provided required notice to individuals.	March 2019

### Observation 4

#### Methods of collection are not reviewed by ATIPP Coordinator prior to implementation

- New collection methods are not reviewed to ensure they are fair and lawful.
- New collection methods are not reviewed to ensure only information needed for its purpose is being collected. A privacy impact assessment is not performed.

#### Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Recommendations:

We recommend that:

- A procedure be formalized that requires all new methods of information collection be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized which specifies actions to be taken by the ATIPP Coordinator to validate only information needed is collected through fair and lawful means.
- A privacy impact assessment be performed for all new information collection methods or changes to existing methods.

### Management Response:

Action Plan	Completion Date:
ENR Corporate Services will inform all divisions of a procedure to complete the Preliminary Privacy Screening Tool any time any new method of information collection is to be enacted. It will be reviewed and approved by the ATIPP Coordinator. A procedure will be formalized that specifies that during their review the ATIPP Coordinator ensures only information needed for its use are being collected, and it is being collected fairly and lawfully. The privacy impact assessment tool is under development by the Dept. of Justice and ENR will comply with any procedures/policies as dictated by the Dept. of Justice to its enactment.	March 2019/as completed by Dept. of Justice.

### Observation 5

#### Procedures do not exist to ensure only information needed is collected

- Existing methods of collection are not reviewed by ATIPP Coordinator along with key stakeholders as required to ensure only information needed is being collected.

### Risk Profile:

Risk Impact	If additional information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office



# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Recommendations:

We recommend that:

- The department reevaluate and reassess the current information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

### Management Response:

Action Plan	Completion Date:
In conjunction with Observations 2 and 3, ENR Corporate Services will review to reevaluate/reassess current information collection needs to support the department mandate. Personal information essential for collection will be distinguished from optional information for each program where personal information collection is required. Existing forms will be reviewed against documented personal information essential for use, and changed as necessary to collect only the information required. As part of this process, Corporate Services will initiate a procedure for form renewal, i.e. set time lines for revisiting the forms for updating.	March 2020

### Observation 6

#### Information sharing agreements do not exist between ENR and other GNWT departments

- A listing does not exist which details the type of information shared through information sharing agreements, with which departments and for what use.

### Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
Risk Responsibility	Assistant Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Recommendations:

We recommend that:

- A listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from ENR and that the agreements provide instructions or requirements 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.

### Management Response:

Action Plan	Completion Date:
Information sharing agreements needs to be discussed at the GNWT level for policy and procedure. This recommendation should be forwarded to the CIO for consideration. The opinion of ENR is that as long as the information is being used within the purpose of why it was collected, the information belongs to the GNWT, not a specific department. Therefore, sharing between departments is not an issue.	N/A

Management responses were provided by Kate Reid, with a copy to Marcelle Marion, and Susan Craig.

# **APPENDIX F**

## **DEPARTMENT OF FINANCE**

### 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, coordinated all of the work 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 Finance (“Finance”) meets its responsibilities through programs it offers through its divisions of:

- Human Resources;
- Shared Corporate Services;
- Budget, Treasury, and Debt Management;
- Employee Services
- Fiscal Policy;
- Internal Audit Bureau;
- Liquor Revolving Fund; and
- Taxation.

Finance collects personal information through:

- Employment and HR related forms, with information stored in PeopleSoft;
- Payroll related forms;
- Insurance applications;
- Various tax forms; and
- Liquor licensing forms.

The main IT system used for the bulk of personal information in this department is PeopleSoft. There are modules within this system for HR and Finance functions and personal information is entered via this tool.

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).

# DEPARTMENT OF FINANCE

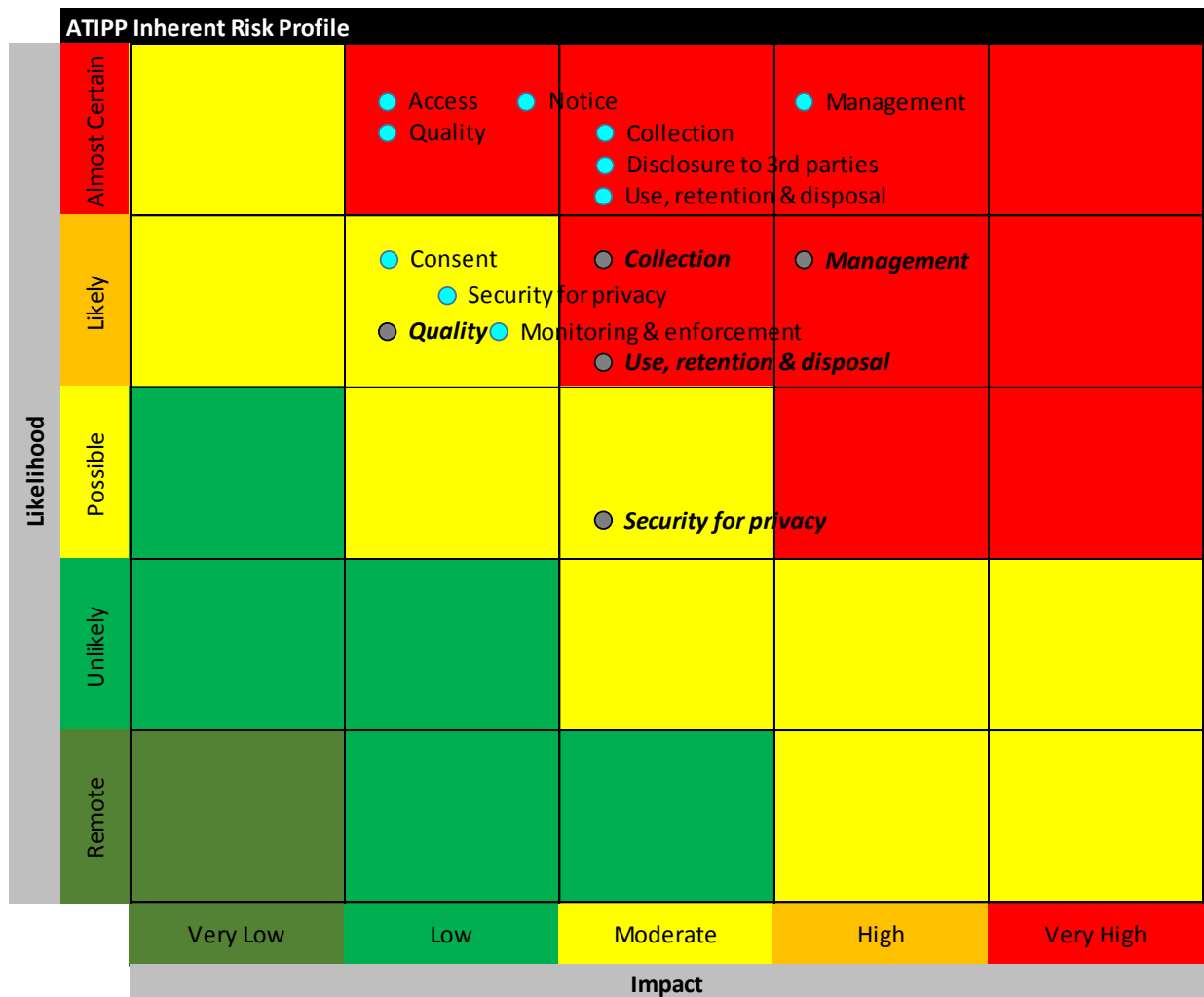
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) PART 2

### Overview

### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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



# DEPARTMENT OF FINANCE

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

### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	NOT COMPLIANT	Contact information and reason for collection is not provided on all forms which require entry of personal information. Principle of collection is not completely met.
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	COMPLIANT	
46	COMPLIANT	
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	COMPLIANT	A full inventory of personal information has not been completed. Full disclosure cannot therefore be verified.
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance..
48	COMPLIANT	
49	N/A	No research use noted
<b>Regulations relating to disclosure of personal information</b>		
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.

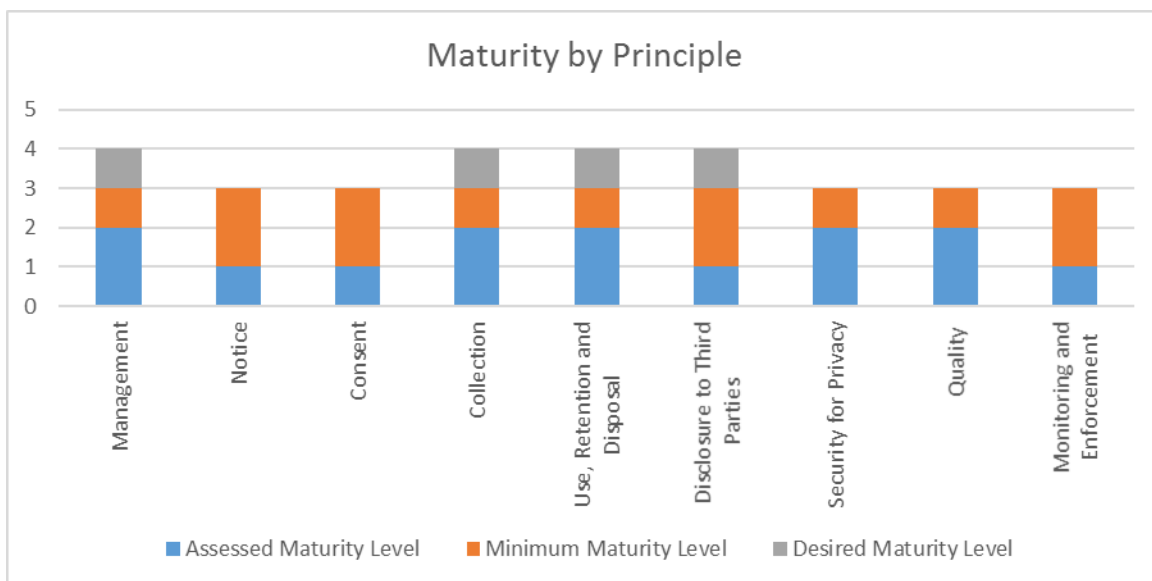
# DEPARTMENT OF FINANCE

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

**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. Finance falls into this category, and is therefore expected to plan for the desired maturity level in the future



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>Although they are able to track the bulk of their personal information by employee name and number, this does not cover all of the areas where personal information is collected and there is no official inventory in place which lists of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP Coordinator has been assigned and has taken the training offered by the Privacy Office. The ATIPP Coordinator is well-versed in privacy legislation and comfortable with the role.</li> </ul>

# DEPARTMENT OF FINANCE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>Privacy Impact Assessments are performed when needed and management works to ensure there is a culture which supports privacy compliance due to the highly confidential nature of the data they work with.</li> </ul> <p><i>See observations 1-2.</i></p>
<p><b>Notice</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms used to collect personal information.</li> </ul> <p><i>See observation 3.</i></p>
<p><b>Consent</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent is obtained on some personal information collection forms but not all. Explicit consent is not obtained.</li> </ul> <p><i>See observation 4.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>Collection of information is limited to the intended use per the use of very detailed forms that request very specific information.</li> <li>A procedure/process does not exist to ensure only information needed is collected.</li> <li>Information obtained by third parties is rare, and when received is disclosed to individual in question</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for.</li> <li>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</li> </ul>



# DEPARTMENT OF FINANCE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>information to be retained for no longer than necessary and is disposed of at that time.</p> <ul style="list-style-type: none"> <li>Information not yet stored in DIIMs is fully managed within other programs with existing use/disposal schedules.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Disclosure to third parties</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>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.</li> <li>Information sharing agreements do not exist with other departments to provide instructions or requirements 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.</li> </ul> <p><i>See observation 6.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place. Physical access to personal information is restricted via close off working spaces and use of locked cabinets for sensitive information.</li> <li>Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>Tests of safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></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"> <li>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.</li> </ul>

# DEPARTMENT OF FINANCE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>Forms used for collecting personal information that is most sensitive in nature have a requirement for the individual to sign off attesting that the data entered is accurate.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></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"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>A process is in place to address inquiries, complaints and disputes.</li> <li>Monitoring and enforcement are being performed on an ad hoc basis at this time – there is no set monitoring of policies or processes to adjust unless a situation arises that draws attention to that process.</li> </ul> <p><i>See observation 5.</i></p>

## Observations and Recommendations

### Observation 1

#### Privacy policy has not been designed and documented

- The responsibility and authority to develop the privacy policies has been unclear.
- The ATIPP Coordinator has limited time and resources to dedicate to ATIPP policies and procedures, specifically in regards to part 2 of the legislation.

#### Risk Profile:

Risk Impact	Without a documented privacy policy, consistent direction cannot be given to departmental personnel which results in inconsistent or lacking 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.

# DEPARTMENT OF FINANCE

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

### Management Response:

Action Plan	Completion Date:
Agreed. The Department of Finance will develop departmental level processes and procedures in conjunction with the development of a GNWT-wide privacy policy and guidelines.  Action: Develop Department of Finance-specific privacy process and procedures to compliment the GNWT-wide privacy policy and guidelines	Fall 2018

### Observation 2

#### An inventory of personal information collected does not exist

- Department staff have knowledge of the personal information collected and are able to track the information that is most sensitive by employee name and number, but a full inventory has not been documented.
- Systems involved in collection and storage of personnel information are not documented.
- Third parties involved are not identified and 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 adequately protected under ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### 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:
Confirmed. The Department will create an inventory of all types of personal information collected to be held by the ATIPP Coordinator. A further review of this inventory will be completed to ensure compliance with the Policy, guidelines and procedures identified in Response #1 above.	

# DEPARTMENT OF FINANCE

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

Action:	
a. Develop inventory of personal information collected.	Fall 2018
b. Review inventory to ensure compliance with policy, guidelines and procedures.	Fall 2018

### Observation 3

#### Forms, hard copy and electronic, used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from some forms.
- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.

#### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to provide the required notice to the individuals.

#### Management Response:

Action Plan	Completion Date:
The Department will undertake a review of all forms (hard copy and electronic) used to collect personal information and where required, update to provide the required notice to individuals.  Action: Review all forms administered by the Department of Finance used to collect personal information and update where required.	Summer 2018

# DEPARTMENT OF FINANCE

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

### Observation 4

#### Not all forms, hard copy and electronic, used to collect personal information require consent from the individual

- Implicit consent is obtained by the individual's signature on the collection form but not all forms require the signature of the individual.
- Explicit consent is not obtained when sensitive information is collected.

#### Risk Profile:

Risk Impact	When consent is not obtained there is an increased risk that full disclosure has not been made; which would result in non-compliance with ATIPP
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to require the individual's signature or explicit consent if sensitive information is being collected.

#### Management Response:

Action Plan	Completion Date:
Agreed. The Department will undertake a review of all forms used to collect personal information and where required, update to receive individual's explicit consent if sensitive information is being collected.  Action: Review all forms used by the Department of Finance to ensure individuals are granting explicit consent when sensitive information is being collected.	Fall 2018

### Observation 5

#### Monitoring, enforcement and updates are being performed on an ad hoc basis

- No set process is in place to regularly monitor the existing processes, to look at effectiveness of controls in place or review for non-compliance.

#### Risk Profile:

Risk Impact	Without scheduled monitoring of policies and processes there is an increased chance of non-compliance with ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

# DEPARTMENT OF FINANCE

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

### Recommendations:

We recommend that:

- A procedure be formalized that requires review of processes to ensure compliance with the department's privacy policies and procedures, laws, regulations and other requirements.

### Management Response:

Action Plan	Completion Date:
Agreed. The Department will establish a procedures to routinely review legislation, regulations and policies to ensure compliance.  Action: Develop an internal procedures to routinely review Finance-specific legislation, regulations and policies to ensure compliance.	Fall 2018

### Observation 6

#### Information sharing agreements do not exist between FINANCE and other GNWT departments

- A listing does not exist which details the type of information shared through information sharing agreements, with which departments and for what use.

### Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
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 listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from FINANCE and that the agreements provide instructions or requirements 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.

# DEPARTMENT OF FINANCE

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

### Management Response:

Action Plan	Completion Date:
<p>Agreed. As part of Action Plan #2 above, the Department will undertake to compile a list of information that is shared with other GNWT departments; and further a list of information that is shared with other GWNT departments, and further ensure information sharing agreements are established with those departments.</p>	
<p>Action:</p> <ul style="list-style-type: none"><li>a. Compile a list of information that is shared with other GWNT departments.</li><li>b. Ensure information sharing agreements are established with departments where information containing personal information is shared.</li></ul>	<p>Fall 2018</p> <p>Fall 2018</p>

Responses were received in a letter signed by David Stewart and copied to Terence Courtoreille.

# **APPENDIX G**

**DEPARTMENT OF HEALTH AND SOCIAL SERVICES**



### 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, coordinated all of the work 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).

# DEPARTMENT OF HEALTH AND SOCIAL SERVICES

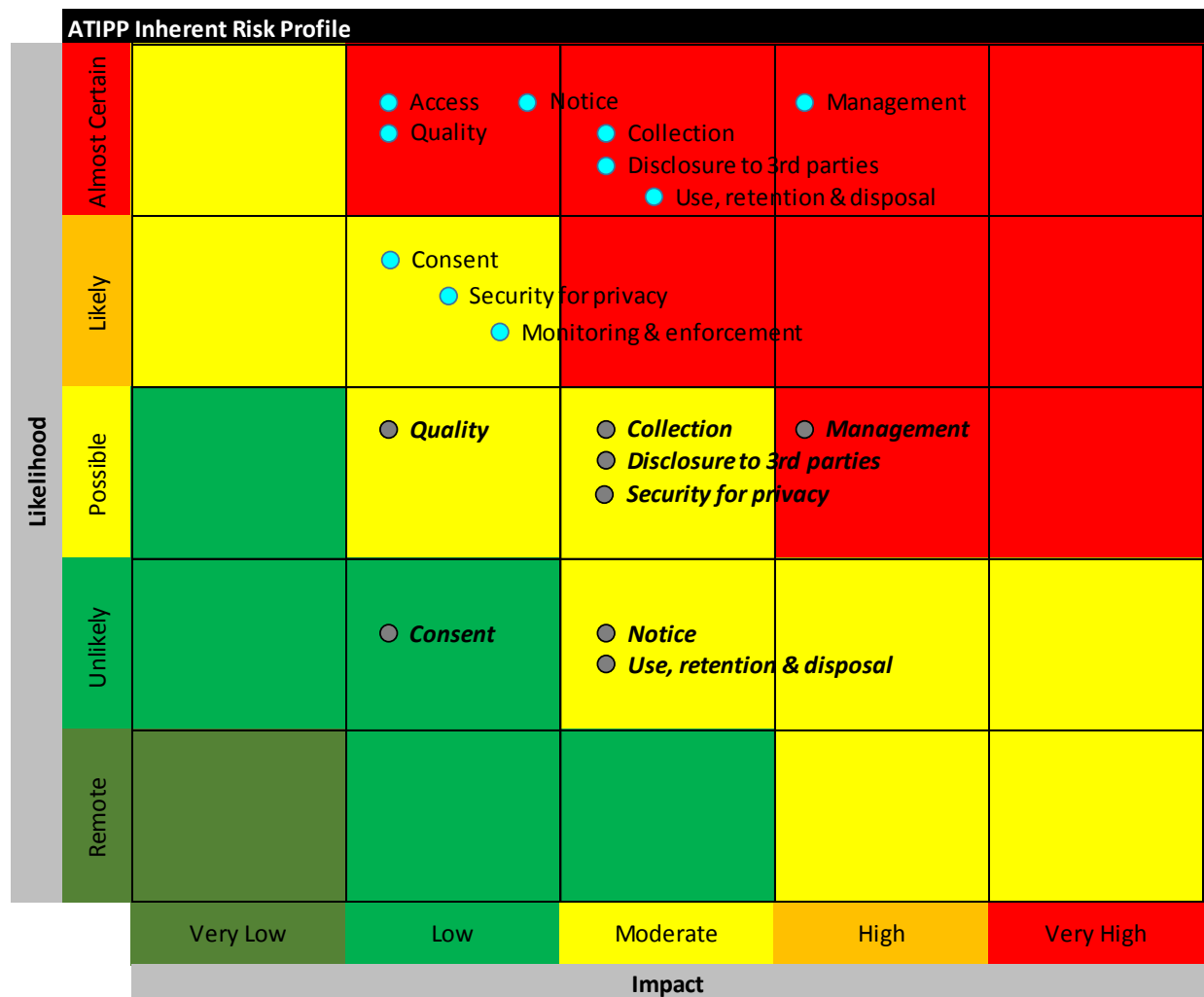
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) PART 2

### 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 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



# DEPARTMENT OF HEALTH AND SOCIAL SERVICES

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

### 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.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
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.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
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.
<b>Regulations relating to disclosure of personal information</b>		
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.

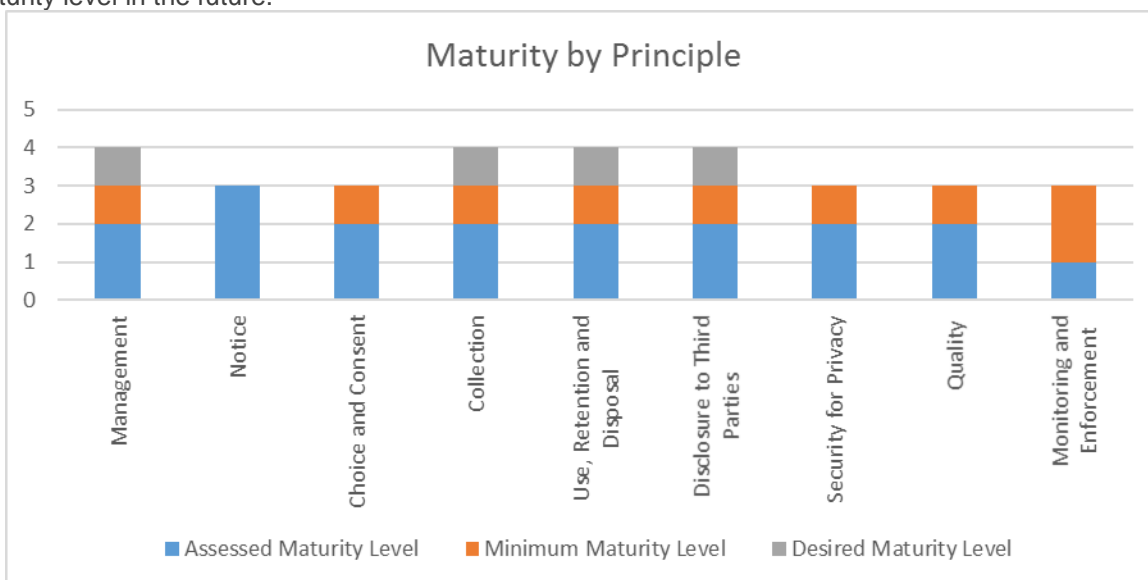
**Minimum Maturity Level** – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

# DEPARTMENT OF HEALTH AND SOCIAL SERVICES

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

**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.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented to address information not legislated by the Health Information Act (HIA).</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP Coordinator has been assigned and works within the department's privacy division.</li> <li>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.</li> <li>Privacy division within department allows for communication of privacy within department and the development of processes to include privacy unit involvement in new programs.</li> </ul>

# 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
		<i>See observations 1-2.</i>
<p><b>Notice</b></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"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is provided on all forms used to collect personal information.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Consent</b></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>	Defined	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent is obtained on personal information collection forms.</li> <li>Explicit consent is obtained on information collection forms when sensitive information is collected.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>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.</li> <li>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.).</li> </ul> <p><i>See observations 1.</i></p>
<p><b>Use, retention and disposal</b></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>	Defined	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process exists to ensure information collected is only used for the purpose it was collected for.</li> <li>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.</li> </ul>

# 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
		<i>See observation 1.</i>
<p><b>Disclosure to third parties</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Information sharing agreements exist with other departments and contracts exist with third parties, to provide instructions or requirements 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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy.</li> <li>• 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.</li> <li>• Physical access to personal information is restricted.</li> <li>• Security measures exist over the transmission of data and are documented.</li> <li>• Tests of all safeguards in place are not performed on a regular basis.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></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"> <li>• 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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> </ul>

# 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
privacy-related complaints and disputes.		<ul style="list-style-type: none"><li>Monitoring and enforcement are not being done at present.</li></ul> <p>See observation 3.</p>

### 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

# DEPARTMENT OF HEALTH AND SOCIAL SERVICES

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

- 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

### 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



# DEPARTMENT OF HEALTH AND SOCIAL SERVICES

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

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. Doing so will ensure the DHSS' procedure will be in line with the new GNWT ATIPP policies.	TBD based on timing of completion of Department of Justice Privacy policies.

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

# **APPENDIX H**

**DEPARTMENT OF INFRASTRUCTURE**

# DEPARTMENT OF INFRASTRUCTURE

## 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, coordinated all of the work 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 Infrastructure meets its responsibilities through programs it offers through its divisions of:

- Asset Management;
- Programs & Services; and
- Regional Operations;

Infrastructure collects personal information through:

- Drivers licensing records;
- Vehicle registration records;
- Fuel sales;
- Building maintenance records;
- Gas inspection records; and
- Contractor records

All divisions expect the Compliance and Licensing Division store personal information collected in hard copy under the Operational Records Classification System and the Administrative Records Classification System and electronic personal information on the Digital Integrated Information Management System (DIIMS). The DRIVES system is used to store all Department of Motor Vehicles personal information, including the driver’s licensing and vehicle registration records noted above.

### Overview

#### Risk Profile

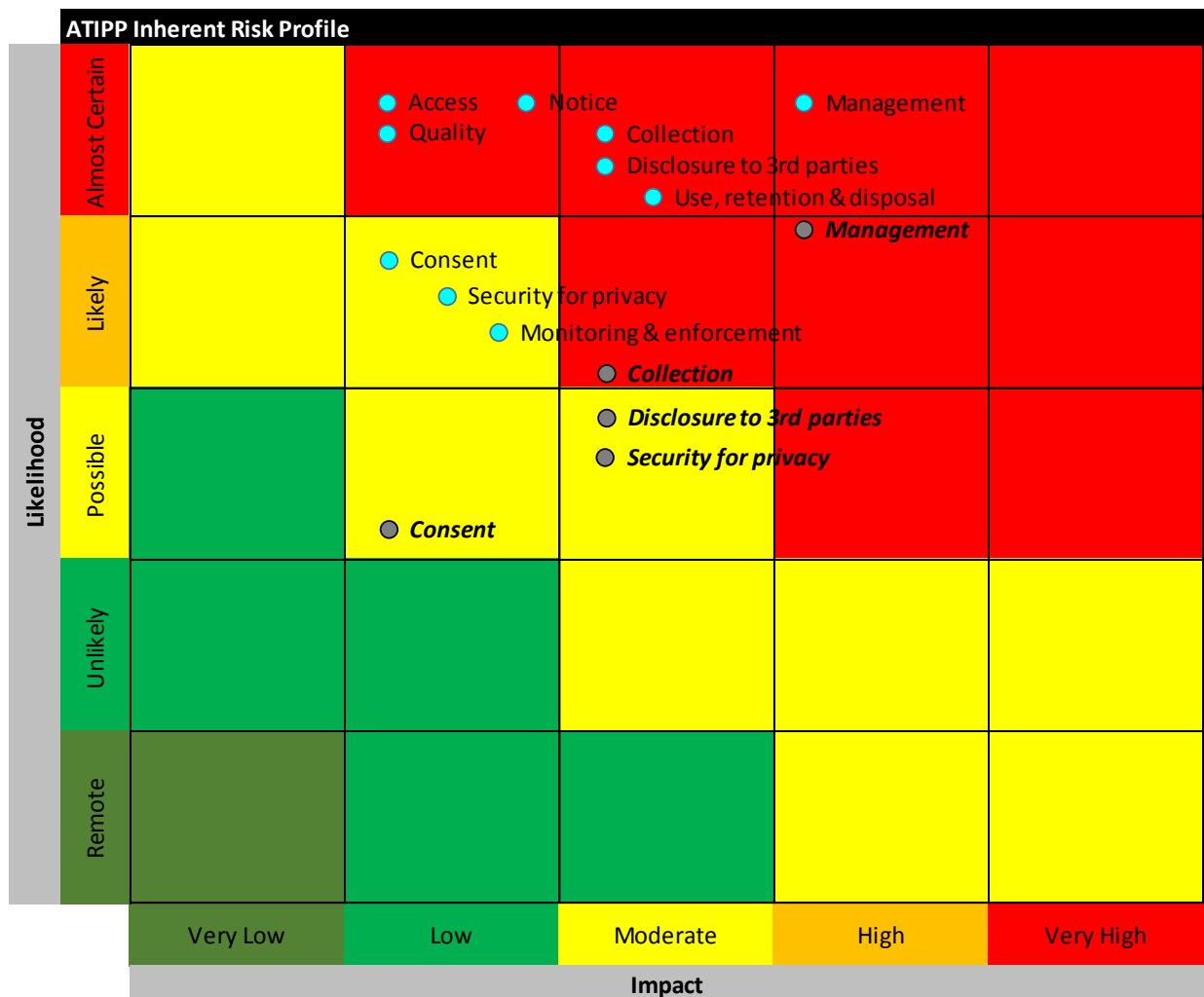
The inherent risk profile per the planning memo, detailed in the chart below, was provided to the department ATIPP Coordinator and privacy contacts at the department interview. The planning risk profile represents

# DEPARTMENT OF INFRASTRUCTURE

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

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 chart 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 location 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 chart below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

# DEPARTMENT OF INFRASTRUCTURE

## 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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	NOT COMPLIANT	Legal authority for collection of personal information and contact information is not provided on all forms. Principle of notice is not completely met.
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	N/A	An error or omission has not been identified.
46	N/A	No requests for correction identified.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	UNVERIFIED	A full inventory of personal information has not been completed. Full disclosure cannot therefore be verified.
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	COMPLIANT	
<b>Regulations relating to disclosure of personal information</b>		
5	COMPLIANT	
6	N/A	No formal examination noted.
8	COMPLIANT	

### 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.

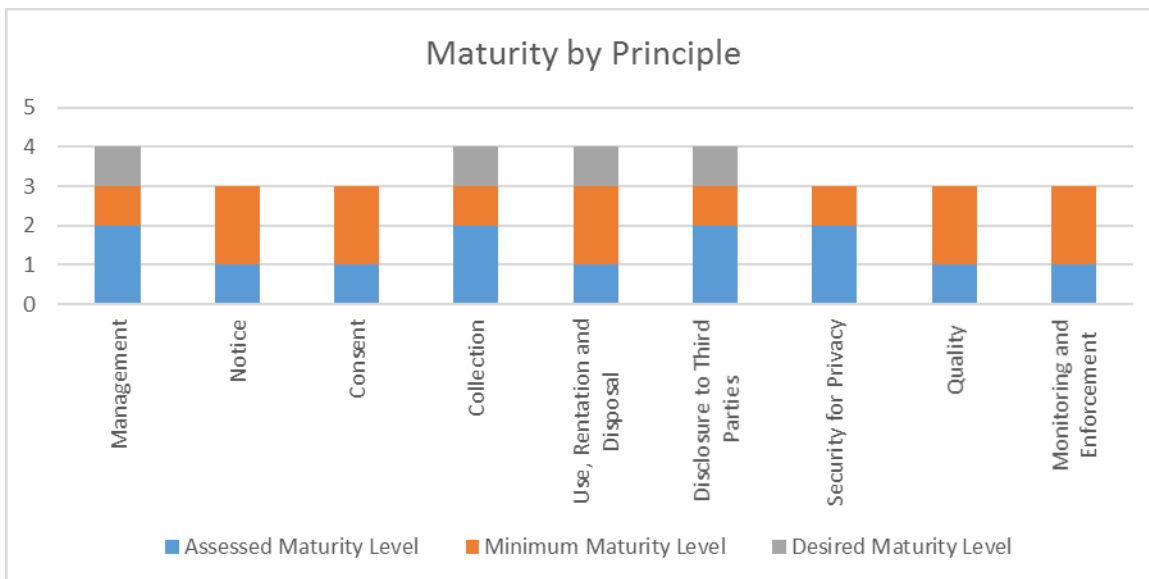
**Minimum Maturity Level** – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

**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.

# DEPARTMENT OF INFRASTRUCTURE

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

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. INF falls into this category, and is therefore expected to plan for the desired maturity level in the future.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Repeatable	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>Procedures around the protection of privacy are largely undocumented</li> <li>An ATIPP Coordinator has been assigned and has taken the training offered by the Privacy Office.</li> <li>Privacy Risk Assessments are completed for all new processes and for old processes if an issue is brought forward.</li> <li>Training material with components of privacy has been developed for staff handling Compliance and Licensing personal information.</li> </ul>
<p><b>Notice</b></p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms (hard copy and online) used to collect personal information.</li> </ul>

# DEPARTMENT OF INFRASTRUCTURE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
personal information is collected, used, retained and disclosed.		<i>See observation 4.</i>
<p><b>Consent</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>• Implicit consent is obtained on forms.</li> <li>• Explicit consent is not obtained on all information forms.</li> </ul> <p><i>See observation 5.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>• The type of personal information collected and the method of collection for personal information collected by forms, in hard copy or online, is known to the individuals.</li> <li>• Personal information from third parties is not accepted except from parties listed under the <i>Motor Vehicles Act</i> section 103 and 104 if a medical professional has grounds to believe the individual cannot operate a vehicle in a safe manner.</li> <li>• Methods and forms of collecting personal information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.</li> <li>• A documented procedure/process does not exist to ensure only personal information needed is collected.</li> </ul> <p><i>See observations 6-8.</i></p>
<p><b>Use, retention and disposal</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>• A documented procedure/process does not exist to ensure personal information collected is only used for the purpose it was collected for.</li> <li>• Retention and disposal of personal information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the DIIMS which allows for personal information to be retained for no longer than necessary and is disposed of at that time, however not all documents have been moved over after the amalgamation of departments.</li> <li>• DRIVES is used to store all Compliance and Licensing personal information. DRIVES has no disposal dates programed, all historical data is being held indefinitely.</li> </ul>

# DEPARTMENT OF INFRASTRUCTURE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<i>See observation 7.</i>
<p><b>Disclosure to third parties</b></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>	Repeatable	<ul style="list-style-type: none"> <li>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 personal information was misused by the third party.</li> <li>Information sharing agreements are in place with the exception of Statistics Canada. GNWT Legal Counsel was used in determining information sharing agreements were not necessary to provide personal information to Statistics Canada.</li> </ul>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>Logical access to personal information is restricted by the department through the use of DIIMS and DRIVES as well as database restrictions put in place.</li> <li>Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>Database access audits are performed to determine if the correct individuals have access.</li> <li>Tests of safeguards in place are performed for the electronic environment.</li> </ul> <p><i>See observation 8.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>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.</li> <li>There is no documented review process in place to ensure new forms developed by staff ensure personal information collected is relevant for the purpose identified.</li> </ul> <p><i>See observation 1 &amp; 6</i></p>
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> </ul>



# DEPARTMENT OF INFRASTRUCTURE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
and has procedures to address privacy-related complaints and disputes.		<ul style="list-style-type: none"> <li>Monitoring and enforcement are not being done at present although there have been reviews of controls in the past. Currently there are no scheduled or regular reviews</li> </ul> <p>See observation 1.</p>

### Observations and Recommendations

#### Observation 1

##### Privacy policy has not been designed and documented

- The responsibility and authority to develop the privacy policies has been unclear.
- Components of privacy protection are within the Driver and Vehicle Licensing Programs but only regarding the Compliance and Licensing personal information. No manual is in place for the other divisions of the department.

#### 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:
<p>The Department of Infrastructure (INF) will work with the Department of Justice to ensure departmental processes and procedures are set up to allow INF to meet the requirements and guidelines of the Government of the Northwest Territories' (GNWT) privacy policy.</p> <p>The Access to Information and Protection of Privacy (ATIPP) Coordinator and ATIPP staff will</p>	<p>INF will be fully compliant with the policy within one year of completion of the policy by the Department of Justice</p>

# DEPARTMENT OF INFRASTRUCTURE

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

<p>ensure that all Senior Managers in INF are aware of the policy and how to be compliant with the policy.</p> <p>All Senior Managers within INF will be provided with a link to the online GNWT ATIPP training to provide to their staff who deal with personal information as part of their jobs. This training which will give these INF employees a basic understanding of the Access to Information and Protection of Privacy Act (ATIPPA).</p>	
--	--

### 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 identified and 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

#### 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:
<p>All INF divisions and regional offices will be asked to provide the INF ATIPP Coordinator with the following information:</p> <ul style="list-style-type: none"> <li>• Every type of personal information collected by the division/office.</li> <li>• The reason for the collection of each piece of personal information.</li> <li>• The method in which that personal information is collected (divisions and regional</li> </ul>	December 1, 2019

# DEPARTMENT OF INFRASTRUCTURE

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

<p>offices will be expected to provide all physical forms, online form, etc.)</p> <ul style="list-style-type: none"> <li>• The staff positions who handle the information from collection to completion.</li> <li>• The process for collection, storage, and deletion of the personal information.</li> <li>• Systems used to collect/store the information.</li> <li>• Third parties who have access to the information.</li> </ul> <p>Once all of this information is collected from each division and regional office, the ATIPP Coordinator will combine the information into one global department inventory.</p> <p>This information will be reviewed by the ATIPP staff to determine if the legislative authority exists for collection of the personal information, if unnecessary personal information is being collected, if the personal information is stored in a secure manner, to ensure only the necessary staff are handling the information, and to ensure the applicable privacy policies are followed.</p>	
--	--

### Observation 3

#### There is a lack of training to support ATIPP within the Department

- 23(2)(d) [redacted] has been requesting the in-depth ATIPP training for approximately one year to better assist the ATIPP Coordinator.

#### Risk Profile:

Risk Impact	Without the proper training programs in place the ATIPP Coordinator cannot properly delegate work to ensue ATIPP compliance.
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:

- Training needs to ensure that there is both awareness and understanding of the full responsibilities of ATIPP compliance

#### Management Response:

Action Plan	Completion Date:
23(2)(d) [redacted] has been asking for the appropriate ATIPP training from the GNWT Access and Privacy Office since INF was formed on April 1, 2017.	As soon as the ATIPP training is made available by the Access and Privacy Office.

# DEPARTMENT OF INFRASTRUCTURE

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

<p>23(2)(d) [REDACTED] has completed the online ATIPP training but requires more in depth training to have a better understanding of the appropriate ATIPP processes and will take the training whenever it is offered by the Access and Privacy Office.</p> <p>All INF staff who deal with personal information will be provided with a link to the online GNWT ATIPP training so they can complete the training and have a basic understanding of the ATIPPA.</p>	
---	--

### Observation 4

#### Forms, hard copy and electronic, used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from most forms.
- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.

#### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to provide the required notice to the individuals.

#### Management Response:

Action Plan	Completion Date:
<p>As indicated under the action plan for Audit Report recommendation number two, the ATIPP Coordinator will ask all INF Senior Managers to provide all forms from their divisions or regional offices on which personal information is collected.</p> <p>Once these forms are compiled the ATIPP staff will review the personal information being collected to determine if it is necessary and that the appropriate legislative authority exists to collect the information. Once this is completed,</p>	December 1, 2019

# DEPARTMENT OF INFRASTRUCTURE

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

<p>each form will be updated to comply with ATIPPA notice requirements, and will include:</p> <ul style="list-style-type: none"> <li>• The purpose for which the information is collected</li> <li>• The specific legal authority for the collection</li> </ul> <p>The title, business address, and business telephone number of an INF staff member who can answer questions about the collection.</p>	
---	--

### Observation 5

#### Not all forms, hard copy and electronic, used to collect personal information require consent from the individual

- Explicit consent is not obtained when sensitive personal information is collected.

#### Risk Profile:

Risk Impact	When consent is not obtained there is an increased risk that full disclosure has not been made, which would result in non-compliance with ATIPP
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to require the individual's signature or explicit consent if sensitive information is being collected.

#### Management Response:

Action Plan	Completion Date:
As part of the collection of forms/information from every division and regional office as indicated under the action plan for Audit Report recommendation number two, once all forms are collected they will be reviewed to determine which ones need to be updated to require an individual's signature/consent for collection of sensitive information.	December 1, 2019

# DEPARTMENT OF INFRASTRUCTURE

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

### Observation 6

#### Program staff develop forms to collect personal information with no documented review process from the ATIPP Coordinator.

- Program staff develops and uses their own forms for the collection of personal information.
- New collection methods are not reviewed to ensure they are fair and lawful.
- New collection methods are not reviewed to ensure only personal information needed for its purpose is being collected. A privacy impact assessment is not performed.

#### Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Director
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 all new methods of personal information collection be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized that specifies that during their review the ATIPP Coordinator ensures only personal information needed for its use are being collected and it is being collected fairly and lawfully.
- A privacy impact assessment should be performed for all significant new personal information collection methods or changes to existing methods.

#### Management Response:

Action Plan	Completion Date:
<p>The ATIPP Coordinator will develop a process that will be distributed to all division and regional offices outlining that all new methods for collection of personal information need to be reviewed and approved by the ATIPP Coordinator. As part of the ATIPP Coordinator's review, every new piece of personal information to be collected will be reviewed to ensure its collection is necessary and that INF has the authority to collect the information. The process will also provide a definition for personal information.</p> <p>The process will also provide that a privacy impact assessment must be completed for all significant new personal information collection methods or changes to existing methods.</p>	December 1, 2019

# DEPARTMENT OF INFRASTRUCTURE

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

### Observation 7

#### Procedures do not exist to ensure only personal information needed is collected

- No documented process exists to ensure only the personal information needed is collected.

#### Risk Profile:

Risk Impact	If additional personal information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- The department documents a process to reevaluate and reassess the current personal information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional personal information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

#### Management Response:

Action Plan	Completion Date:
<p>As part of the action plan for Audit Report recommendation number two, the ATIPP Coordinator will be able to determine what personal information is being collected by every division and regional office, and if that collection is necessary. Once this review is complete, the ATIPP Coordinator will be able to update the process being developed as part of the action plan for recommendation six to establish how often the Department should reevaluate/reassess what personal information is being collected and if that collection is necessary.</p> <p>As part of the action plan for recommendation two, the necessary personal information that is being collected by each division and regional office will be distinguished from the optional personal information that is being collected. All forms will be updated to ensure only the necessary personal information is being collected.</p>	December 1, 2019

# DEPARTMENT OF INFRASTRUCTURE

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

### Observation 8

#### Not all records are held in the Digital Integrated Information Management System (DIIMS) or DRIVES system.

- Records from pre-amalgamation have not fully been moved into the DIIMS.
- The DRIVES system has no disposal date, all historical personal information could be accessed.

#### Risk Profile:

Risk Impact	When records are left in locations that can be accessed there is increased risk that personal information will be seen by people who are not part of the use for which the disclosure was made upon collection. This would result in non-compliance with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- A review of records from pre-amalgamation be performed, and any sensitive personal information not related to the Compliance and Licensing Division, be moved from any identified older insecure systems to DIIMS. If personal information is held in a separate database that is up to date and secure, these items would be left as-is.
- A policy is implemented that outlines the scheduled disposal dates of all documents that are stored in the DRIVES system.
- The DRIVES system is updated to dispose of documents in accordance with ATIPP on the scheduled disposal date, or if it not possible to set up electronically, a manual system be implemented to delete these files.

#### Management Response:

Action Plan	Completion Date:
<p>All INF divisions and regional offices will be asked to review their records to determine if there is sensitive personal information being stored on older systems that may not be secure.</p> <p>All divisions and regional offices, with the assistance of INF Information Technology staff, will need to determine if the databases have controls over who can access documents, if regular maintenance updates are completed, and if security measures are in place to keep the systems physically safe.</p> <p>The network drives are physically secure and do undergo regular maintenance, and it is possible to restrict access to the folders beyond basic</p>	December 1, 2019



# DEPARTMENT OF INFRASTRUCTURE

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

divisional and departmental settings. The Technology Service Centre will be asked to assist with further lockdowns if necessary. If sensitive personal information is found to exist on a system that is not secure, it will be moved into DIIMS.

In regards to the DRIVES system, records kept in this system are required to be maintained for longer periods of time when compared to other INF records. Retention of these records for longer periods is required to properly administer driver and vehicle related programs and the Motor Vehicles Act.

The Compliance and Licensing Division will develop a process that will require the Division to meet annually to determine if there are areas in DRIVES in which significant amounts of information/records are being maintained when there is no longer a purpose for them under the Motor Vehicles Act and associated regulations/programs. The process will also outline how such records would then be deleted.

Responses were provided via email with a copy to Sonya Saunders and were approved by the department Deputy Minister.

# **APPENDIX I**

**DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT**

### 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, coordinated all of the work 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 Industry, Tourism and Investment (“ITI”) meets its responsibilities through programs under its divisions of:

- Minister’s Office;
- Directorate;
- Finance and Administration;
- Policy Legislation and Communications;
- Business Support, Trade and Economic Analysis (Trade and Investment, Trade and Business Immigration, Economic Analysis, The BIP Monitoring Office);
- Economic Diversification (NWT Film Commission, Arts and Fine Crafts, Traditional Economy, Project Support);
- Tourism and Parks;
- Diamonds, Royalties and Financial Analysis;
- Client Service and Community Relations;
- Mineral Resources; Industrial Initiatives;
- Mining Recorder’s Office; Petroleum Resources;
- Northwest Territories Geological Survey; and
- Regions:
  - Inuvik Region;
  - Dehcho Region;
  - North Slave Region;
  - South Slave Region;
  - Sahtú Region.

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

ITI collects personal information through:

- Oil and Gas Subsurface Tenure Management – Petroleum LAS database;
- Loan and Grant Management – TEA database;
- Business Incentive Program registry – BIP Registry;
- Mineral Information Tenure System – MITS database;
- Mineral Resource Act Engagement – MRA Engagement System; and
- Petroleum Resource Act Engagement – PRA Engagement System.

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

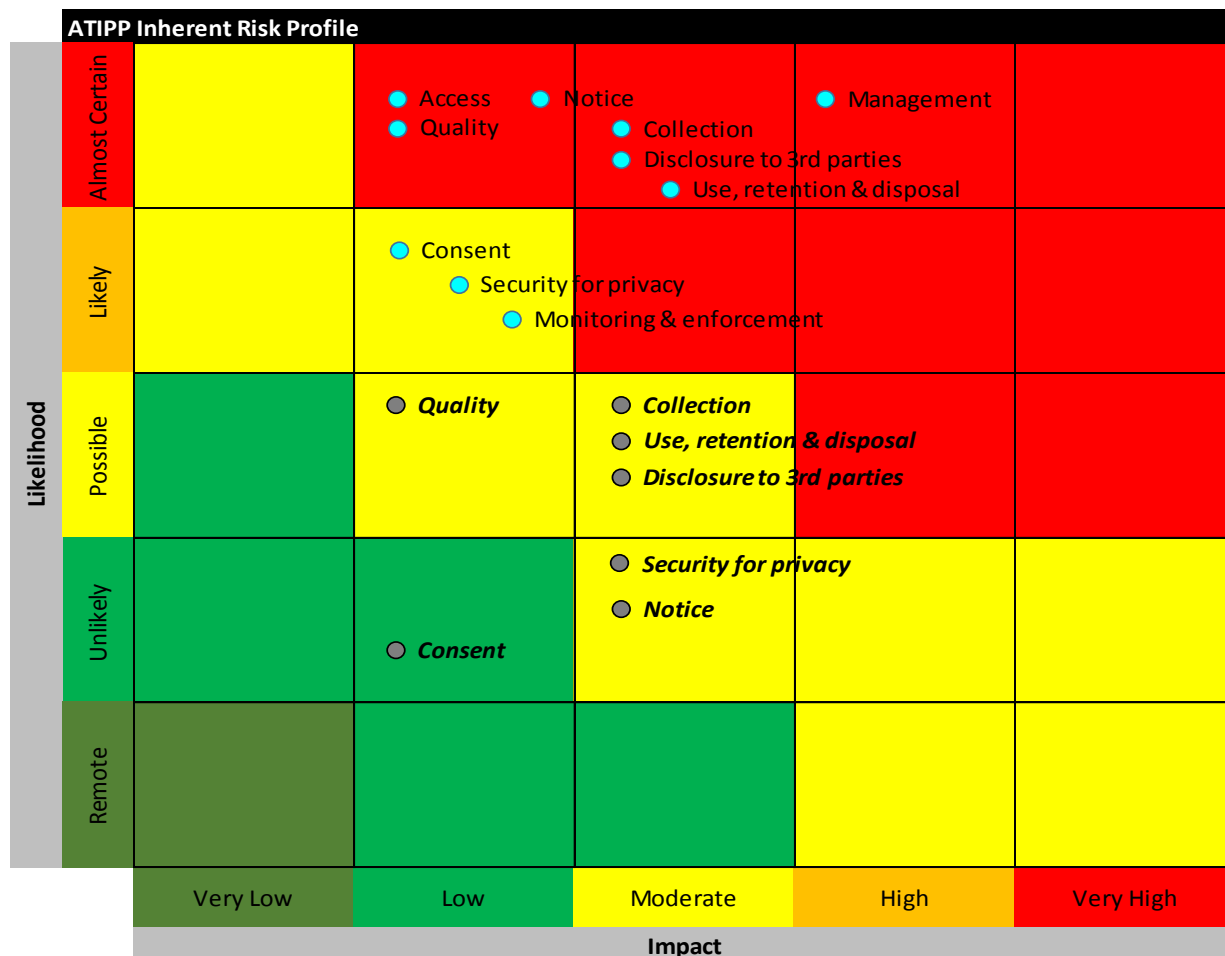
#### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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.

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

### RISK HEATMAP



### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	COMPLIANT	

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

Section	Compliance Assessment	Reason for Non-Compliance
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
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.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	COMPLIANT	
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	N/A	No research use noted.
<b>Regulations relating to disclosure of personal information</b>		
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.

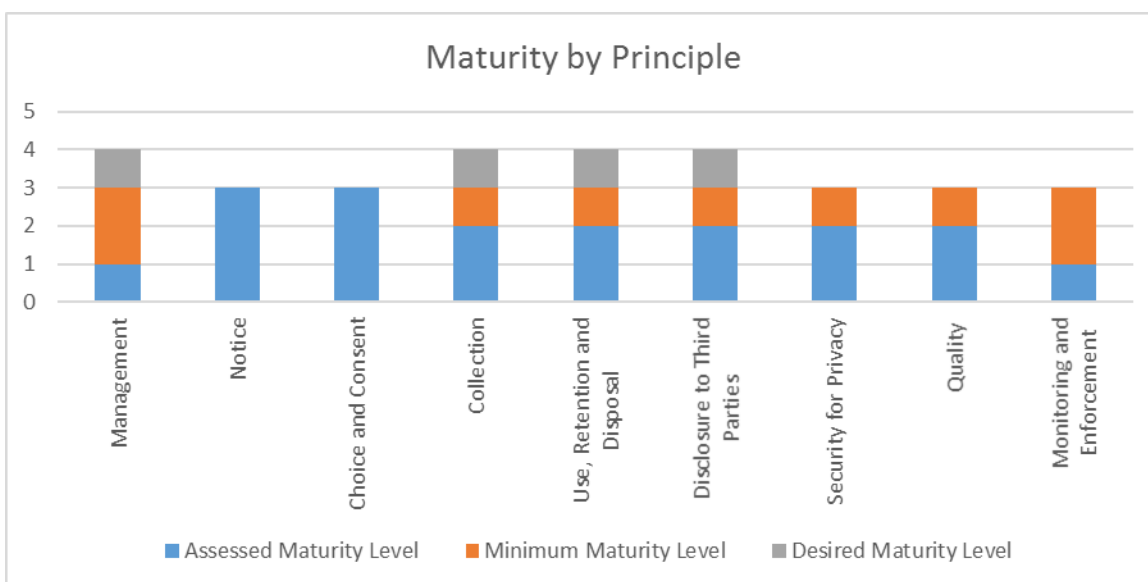
**Minimum Maturity Level** – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

**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.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As ITI does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

## 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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>There is a strong departmental culture over personal information through informal communications.</li> <li>An ATIPP Coordinator has been assigned.</li> <li>ATIPP Coordinator is familiar with ATIPP and has resources to address ATIPP requirements.</li> <li>Privacy Impact Assessments (“PIAs”) are not been done at present.</li> </ul> <p><i>See observations 1-3.</i></p>
<p><b>Notice</b></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"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms (hard copy and online) used to collect personal information.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Consent</b></p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect</p>	Defined	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> </ul>

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
to the collection, use and disclosure of personal information.		<ul style="list-style-type: none"> <li>Explicit consent is obtained on information collection forms.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>The type of personal information collected and the method of collection for personal information collected by forms is known to the individual.</li> <li>The department does not disclose the collection of information through the use of cookies.</li> <li>Information is collected from third parties and developed or acquired about the individual for which the individual is notified and consent is obtained.</li> <li>Methods and forms of collecting information are provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means and only information needed is collected.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process does exist to ensure information collected is only used for the purpose for which it was collected.</li> <li>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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Disclosure to third parties</b></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>	Repeatable	<ul style="list-style-type: none"> <li>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.</li> <li>Information sharing agreements and contracts exist with departments and third parties to provide instructions or requirements to the departments regarding the personal information disclosed, to ensure the information is only</li> </ul>



# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>used for the purpose for which it was collected and the information will be protected consistent with the department's requirements.</p> <p><i>See observation 1.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Shares Services Centre.</li> <li>• Physical access to personal information is restricted through access to building, floor restriction access, storage in secure and locked cabinets.</li> <li>• Security measures over the transmission of data are not formally designed.</li> <li>• Tests of all safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></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"> <li>• 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.</li> <li>• Accuracy and completeness is confirmed by individual through signature on forms</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></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"> <li>• A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>• Monitoring and enforcement are not being done at present.</li> </ul> <p><i>See observation 1.</i></p>

### Observations and Recommendations

#### Observation 1

##### Privacy policy has not been designed and documented

- Procedures and forms have been used to address privacy matters. There is not a fully documented privacy policy in place.

##### 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:
We are supportive of the development of a GNWT-wide policy and will assist with its implementation as suggested. There is limited work we can do however until such a policy is made.	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 containing personal information are correctly protected under ATIPP.
Risk Responsibility	Director

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office
-------------------------	---

### 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:
We will be asking all our divisions that manage and collect personal information to begin tracking and recording their personal information in a protected location. We will also ask them to share this information with our ATIPP Coordinator via a global departmental inventory. The rollout of the departmental inventory will be led and directed by our ATIPP Coordinator, who will also be responsible for ensuring that adequate compliance processes and procedures are in place at each of these data transmission points and that the completeness and security of the inventory is maintained on an ongoing basis.	Work on the inventory will be ongoing, but a substantial amount of the work needed to establish the inventory will be done by September 2018.

### Observation 3

#### More support is needed by ATIPP within the Department to increase maturity of ATIPP processes

- Strong understanding of ATIPP requirements and importance of privacy of personal information collected, used and retained by ATIPP Coordinator
- Resources within the Legislation and Legal Affairs division are responsible for matters other than ATIPP and therefore time constraints reduce their ability to implement more mature processes such as privacy impact assessments.

### Risk Profile:

Risk Impact	Without a set role with assigned responsibilities as outlined in a job description, the privacy function (whether part of another role or in its own capacity) will be limited in ability to fulfill the role.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

# DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

### Recommendations:

We recommend that:

- The roles and responsibilities of the ATIPP Coordinator be defined, addressing both ATIPP Part 1 and Part 2
- The department should evaluate capacity and capability of current resources. Awareness of resources for ATIPP understanding, training and guidance is required along with support for ATIPP compliance activities.

### Management Response:

Action Plan	Completion Date:
We will begin to develop internal awareness materials which clarify best practices and the responsibilities of staff and the ATIPP Coordinator for ensuring ATIPP compliance. Work will take into account current resourcing constraints in ITI and the DOJ's tentative plans to centralize ATIPP coordinators, will be coordinated with the DOJ Access and Privacy Office	Options to strengthen ATIPP resources within ITI will be contemplated over this fiscal year and the next, subject to the GNWT fiscal planning cycle.

Responses provided by Natasha Brotherston with copies to Nick Leeson and Bianca Masalin-Basi.

# **APPENDIX J**

## **DEPARTMENT OF LANDS**

### 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, coordinated all of the work 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 Lands (“Lands”) was created in April 2014, transferring public land management and administration functions from the federal government for Territorial lands and from the GNWT Department of Municipal and Community Affairs for Commissioner’s Lands. Lands meets its responsibilities through programs it offers through its divisions of:

- Directorate;
- Finance and Administration;
- Informatics Shared Services;
- Commissioner’s and Territorial Land Administration;
- Land Use and Sustainability;
- Policy, Legislation and Communications;
- Regional offices; and
- Securities and Project Assessment.

Lands collects personal information through:

- Commissioner’s and Territorial Land Administration
- Informatics Shared Services Centre

Personal information collected as part of Land Administration is stored in the LIMS database – Lands Lease Information Management System, LAS – Commissioner’s Lands Lease Administration System, IRRA – Inspection Risk Reporting Analysis program, and ATLAS (Administration of the Territorial Land Acts System).

The NWT Centre for Geomatics in the Informatics Shared Services Centre collects names, addresses and email information from users wishing to download geospatial information from their website as some

# DEPARTMENT OF LANDS

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

datasets are under a specific license agreement. This information is stored in an MS SQL database which has restricted access to three individuals.

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

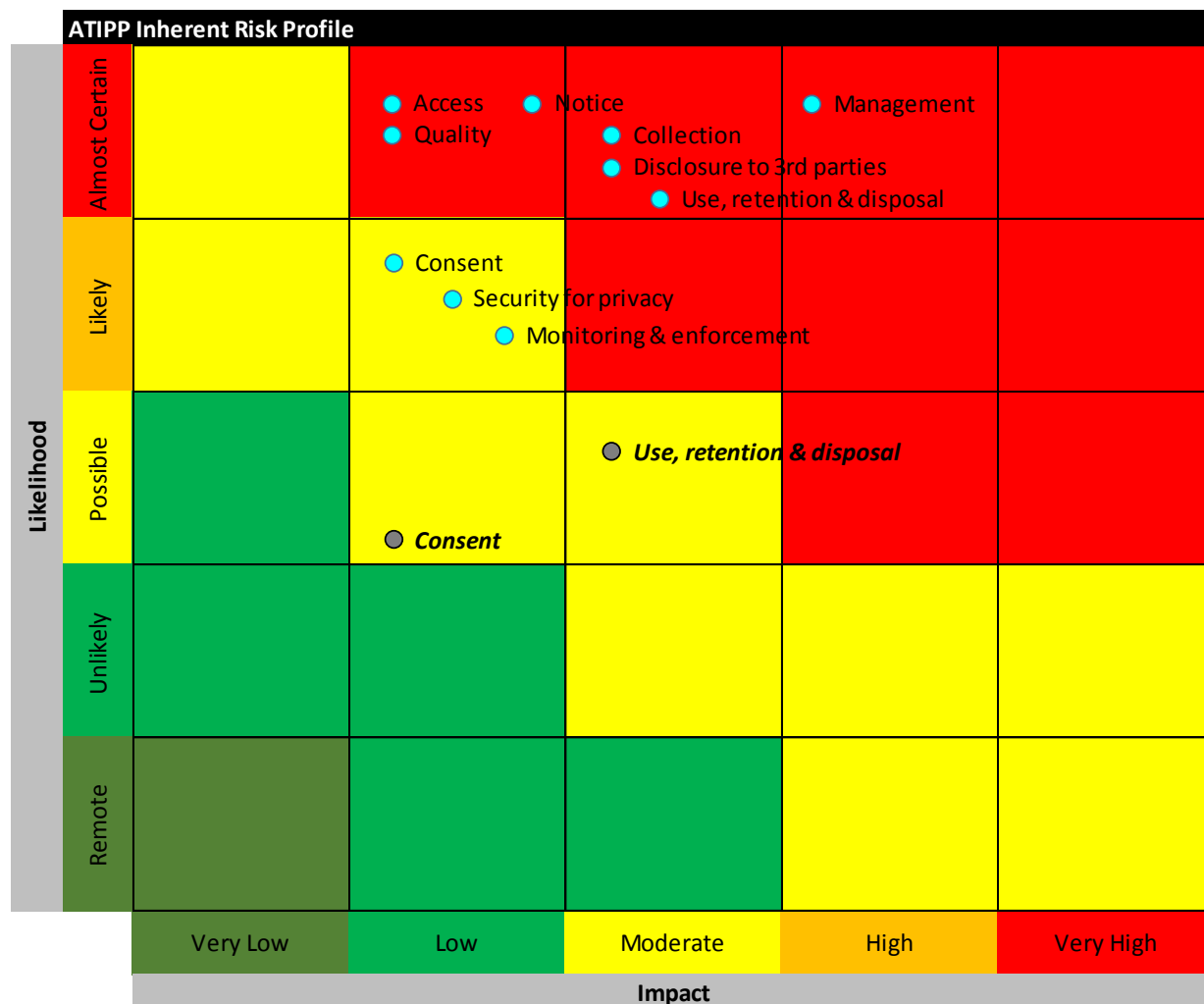
#### Risk Profile

The inherent risk profile per the planning memo, detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the AICPA/CICA Privacy Maturity Model Principles. 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 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.

# DEPARTMENT OF LANDS

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

### RISK HEATMAP



### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation has been made. Further details of these compliance requirements are outlined in Appendix A. The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	



# DEPARTMENT OF LANDS

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

Section	Compliance Assessment	Reason for Non-Compliance
41 (2) & (3)	NOT COMPLIANT	Legal authority for collection of information and contact information is not provided on all forms. Principle of notice is not completely met.
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	COMPLIANT	
46	N/A	A disclosure has not been identified.
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	COMPLIANT	
47.1	COMPLIANT	No reporting received to date to indicate non-compliance.
48	COMPLIANT	
49	N/A	No research use identified
<b>Regulations relating to disclosure of personal information</b>		
5	COMPLIANT	
6	N/A	No formal examination noted.
8	N/A	No research agreement in place.

### Maturity Rating against Privacy Maturity Model

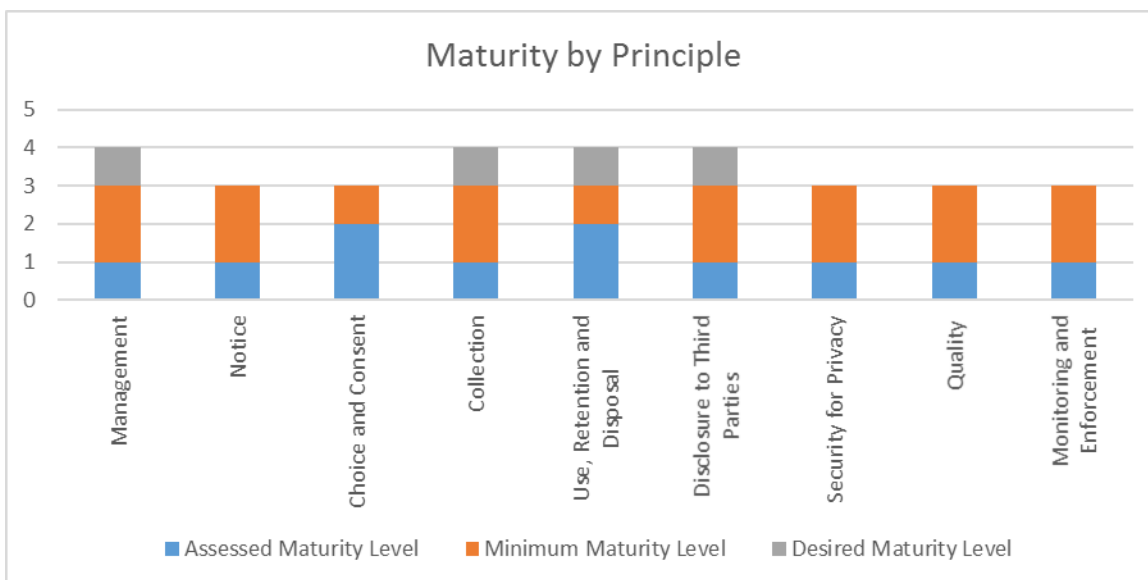
Using the Privacy Maturity Model (**Appendix A refers**), the assessed maturity, minimum maturity and desired maturity are illustrated in the graph below.

**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.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As Lands does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.



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><b>Management</b></p> <p>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>There is a strong departmental culture over personal information through informal communications.</li> <li>An ATIPP Coordinator has been assigned.</li> <li>ATIPP Coordinator has been waiting to take the training sessions offered by the Privacy Office.</li> <li>Privacy Impact Assessments do not appear to be used at this time</li> </ul> <p><i>See observations 1-3.</i></p>
<p><b>Notice</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms used to collect personal information.</li> </ul> <p><i>See observation 4.</i></p>
<p><b>Consent</b></p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> </ul>

# DEPARTMENT OF LANDS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
to the collection, use and disclosure of personal information.		<ul style="list-style-type: none"> <li>• Implicit consent is obtained on personal information collection forms.</li> <li>• Explicit consent is obtained on information collection forms.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>• The type of personal information collected and the method of collection for personal information collected by forms is known to the individual.</li> <li>• Personal information is not collected by third parties.</li> <li>• Methods and forms of collecting information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.</li> <li>• A procedure/process does not exist to ensure only information needed is collected.</li> </ul> <p><i>See observations 5-6.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>• There are security provisions in place to ensure that data cannot be pulled and used for purposes other than that for which it was collected, but there are no documented processes in place to ensure information collected is only used for the purpose for which it was collected</li> <li>• 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.</li> </ul> <p><i>See observation 5.</i></p>
<p><b>Disclosure to third parties</b></p> <p>The department discloses personal information to third parties only for the purposes identified in the notice and</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be</li> </ul>

# DEPARTMENT OF LANDS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
with the implicit or explicit consent of the individual.		<p>taken if the information was misused by the third party.</p> <ul style="list-style-type: none"> <li>Information sharing agreements do not exist with other departments to provide instructions or requirements 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.</li> <li>Policy exists that provides guidance on how to address requests for lease information from lenders.</li> </ul> <p><i>See observation 7.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address security for privacy.</li> <li>The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Shared Services Centre.</li> <li>Physical access to personal information is restricted through access to building, floor restriction access, storage in secure and locked cabinets.</li> <li>Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>Tests of all safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>Monitoring and enforcement are not being done at present.</li> </ul>

# DEPARTMENT OF LANDS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
privacy-related complaints and disputes.		<i>See observation 1.</i>

### Observations and Recommendations

#### Observation 1

##### Privacy policy has not been designed and documented

- When the department was created in 2014 the policies and procedures of the federal and territorial functions assumed were adopted, which did not include specific privacy policies.
- The policies have not been reviewed nor updated since the department was created in regards to privacy, specifically ATIPP part 2.

#### 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:
<p>The Department of Justice is in the process of developing a GNWT-wide Protection of Privacy Policy. The draft Policy has been shared with all departments for review and discussion. It is anticipated that the Policy will be finalized by June 30, 2018.</p> <p>The draft Protection of Privacy Policy is part of an overarching GNWT Privacy Framework that is being developed to support departments in ensuring that the privacy provisions of the ATIPP Act are administered in a consistent and fair manner. The framework will include guidelines to</p>	December 2018

# DEPARTMENT OF LANDS

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

assist departments in developing their own privacy management programs. The Department of Justice anticipates finalizing the Privacy Framework by June 30, 2018 and will be working with departments to implement the framework across the GNWT over the summer/fall of 2018.	
---	--

### 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 personal 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 containing personal information are correctly protected under ATIPP.
Risk Responsibility	All Divisional directors/Superintendents and the ATIPP Coordinator
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### 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:
The Department will develop a global inventory of all the types of personal information and the related processes and systems. Each divisional director will be responsible to provide the information to the ATIPP Coordinator.	October 2018
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the ATIPP Coordinator will conduct an internal review to ensure compliance processes and procedures are in place.	March 2019

### Observation 3

#### There is a lack of support provided to ATIPP within the Department

- ATIPP Coordinator has not been able to take the three-day in-depth ATIPP training by the Privacy Office; currently the knowledge level is inadequate to allow this individual to effectively complete their full ATIPP responsibilities.
- Job description of the ATIPP Coordinator, who is also the Director, Policy, Legislation and Communications outlines responsibilities for only Part 1 of ATIPP responsibilities and not Part 2.

#### Risk Profile:

Risk Impact	Without a set role with assigned responsibilities as outlined in a job description, the privacy function (whether part of another role or in its own capacity) will be limited in ability to fulfill the role. Without additional avenues for training, there is increased risk that the privacy Coordinator may not have the full understanding required to carry out the role.
Risk Responsibility	Deputy Minister and Assistant Deputy Minister Planning and Coordination
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- The roles and responsibilities of the ATIPP Coordinator be defined, addressing both ATIPP Part 1 and Part 2
- Training for ATIPP Coordinator be reviewed and adjusted as needed to ensure that there is both awareness and understanding of the full responsibilities of ATIPP compliance. This will allow for better provision of guidance to the department.
- The department should evaluate capacity and capability of current resources. Awareness of resources for ATIPP understanding, training and guidance is required along with support for ATIPP compliance activities.

#### Management Response:

Action Plan	Completion Date:
The Job Description for the Director, Policy Legislation and Communications position will be amended to include responsibilities under Part 1 and Part 2 of the ATIPP Act and reevaluated by HR.	July 2018

### Observation 4

#### Forms used to collect personal information are not consistently providing the required notice

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from forms were used for GNWT functions prior to the creation of Lands.

# DEPARTMENT OF LANDS

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

- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.
- Forms used for functions that were Federal government functions prior to the creation of Lands contain the required notice.

### Risk Profile:

Risk Impact	Lack of notice on forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director Commissioner's Land Administration
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- All forms used to collect personal information be reviewed and updated to consistently provide the required notice to individuals.

### Management Response:

Action Plan	Completion Date:
The Department will review and amend the Application Forms for Commissioner's Land to include the privacy notice and ensure that the forms are compliant with Part 2 of the ATIPP Act.	May 2018

### Observation 5

#### Methods of collection are not reviewed by ATIPP Coordinator prior to implementation

- New collection methods are not reviewed to ensure they are fair and lawful.
- New collection methods are not reviewed to ensure only information needed for its purpose is being collected. A privacy impact assessment is not performed.

### Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is an increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Delegated ATIPP Coordinator and all Divisional Directors/Superintendents
Risk Mitigation Support	The office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- A procedure be formalized that requires all new methods of information collection to be reviewed and approved by the ATIPP Coordinator.



# DEPARTMENT OF LANDS

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

- A procedure be formalized which specifies actions to be taken by the ATIPP Coordinator to validate only information needed is collected through fair and lawful means.
- A privacy impact assessment should be performed for all new information collection methods or changes to existing methods.

### Management Response:

Action Plan	Completion Date:
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the ATIPP Coordinator will develop a directive/procedure for all Divisions to submit any new method of information collection for review and assessment. The directive will include the requirement for all divisions to conduct a privacy impact assessment as part of the package to be reviewed.	March 2019

### Observation 6

#### Procedures do not exist to ensure only information needed is collected

- Existing methods of collection are not reviewed by the ATIPP Coordinator along with key stakeholders as required to ensure only information needed is being collected.

### Risk Profile:

Risk Impact	If additional information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- The department reevaluate and reassess the current information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

### Management Response:

Action Plan	Completion Date:
Once the new GNWT Privacy Management Program is in place and the Department has the	March 2019

# DEPARTMENT OF LANDS

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

<p>tools and guidelines it needs, the Director of Commissioner’s Land Administration and the Director of Territorial Land Administration will review and reevaluate the information that is being collected to ensure that only essential information is being collected. Based on the review, the application forms will be amended accordingly, if necessary.</p> <p>The NWT Genomatics Centre is currently reviewing the need to collect personal information from users that download geospatial datasets</p>	<p>October 2018</p>
---	---------------------

### Observation 7

#### Information sharing agreements do not exist between LANDS and other GNWT departments

- A listing does not exist which details the type of information shared through information sharing agreements, with which departments and for what use.

#### Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
Risk Responsibility	Assistant Deputy Minister Operations, Executive Director Informatics Shared Services Centre, and Director Finance and Administration
Risk Mitigation Support	All Divisional Directors, the Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- A listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from LANDS and that the agreements provide instructions or requirements 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.

# DEPARTMENT OF LANDS

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

### Management Response:

Action Plan	Completion Date:
The Department will develop a listing of all the private information that is shared with other GNWT Departments, and review its necessity for being shared.	October 2018
Once the new GNWT Privacy Management Program is in place and the Department has the tools and guidelines it needs, the Department will draft and enter into information sharing agreements with the other GNWT departments.	March 2019

Responses provided by Shauna Hamilton with copies to Brenda Hilderman, Shelly Kavanagh and Kate Hearn.

# **APPENDIX K**

**DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS**

### 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, coordinated all of the work 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 Municipal and Community Affairs (“MACA”) meets its responsibilities through programs it offers through its divisions of:

- Office of the Fire Marshall;
- Emergency Management;
- Consumer Affairs & Licensing;
- Sport, Recreation, Youth & Volunteerism;
- Community Governance Support and Advice; and
- Training - School of Community Government.

MACA collects personal information through:

- Office of the Fire Marshall, which is stored on the FDM database;
- Training - School of Community Government division, which is stored on the Student Database and eLearning database;
- Community Governance Support and Advice division, which is stored on the Computer Assisted Mass Appraisal (CAMAlot) database
- Consumer Affairs & Licensing division; and
- Sport, Recreation, Youth & Volunteerism division.

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).

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

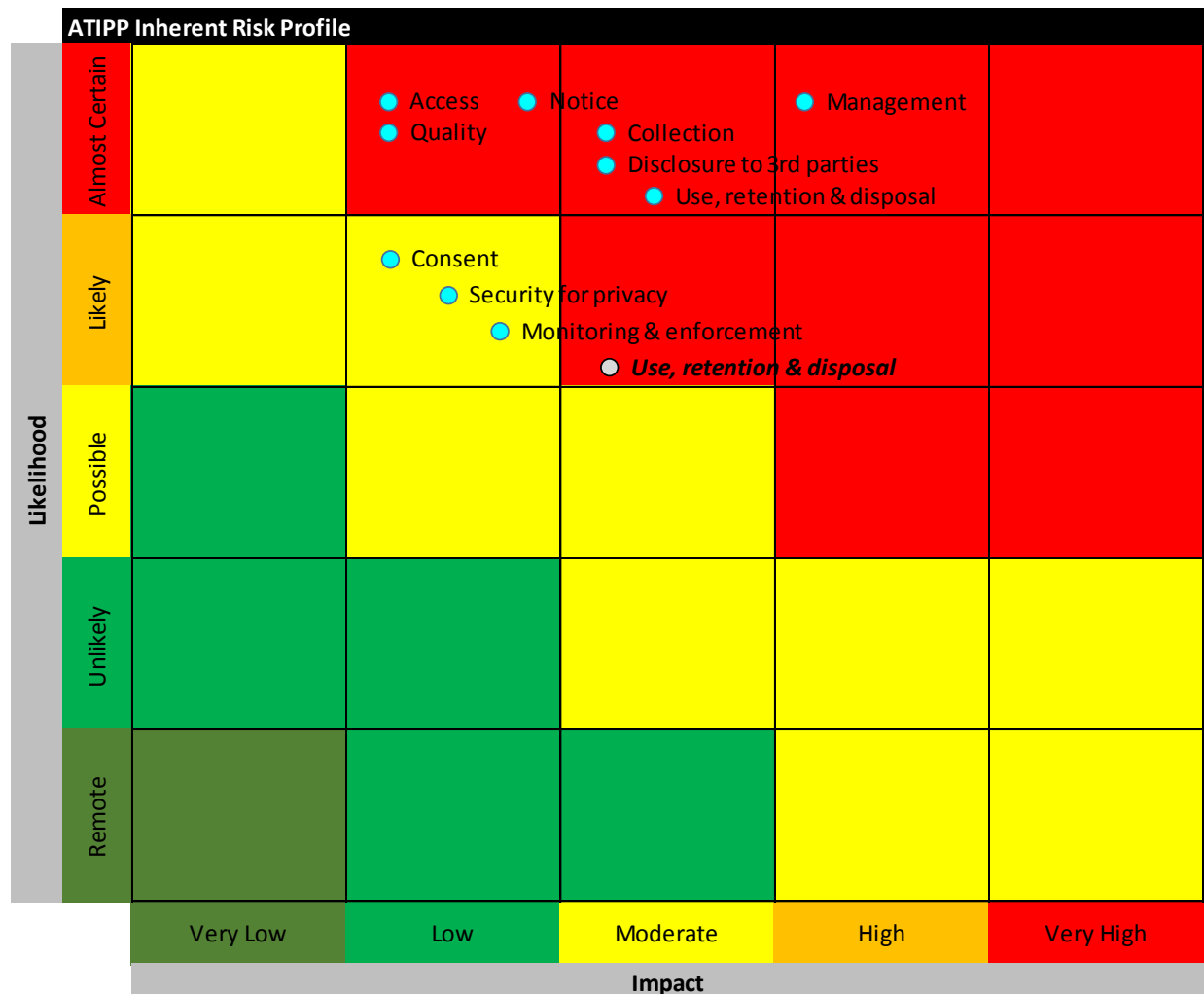
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) PART 2

### Overview

#### Risk Profile

The inherent risk profile detailed in the risk heatmap below, was provided to the department ATIPP Coordinator and privacy contacts during the department interview. The planning risk profile represents our view of the inherent risks for GNWT based on the IAB's risk rating criteria as applied to the Privacy Maturity Model Principles. The heatmap shows the initial inherent risk rating for each principle in regular black print as well as our assessed 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



# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Compliance with ATIPP Part 2 Protection of Privacy

An assessment of compliance with the specific requirements of ATIPP legislation was made (**Schedule 2 refers**). The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant.

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

Section	Compliance Assessment	Reason for Non-Compliance
<b>Part 2: Division A – Collection of Personal Information</b>		
40	COMPLIANT	
41 (1)	COMPLIANT	
41 (2) & (3)	NOT COMPLIANT	Contact information is not provided on all forms. Principle of collection is not completely met.
42	COMPLIANT	
<b>Part 2: Division B – Use of Personal Information</b>		
43	COMPLIANT	
44	COMPLIANT	
45	COMPLIANT	
46	COMPLIANT	
<b>Part 2: Division C – Disclosure of Personal Information</b>		
47	UNVERIFIED	A full inventory of personal information has not been completed. Full disclosure cannot therefore be verified.
47.1	UNVERIFIED	Cannot confirm a negative, therefore unverifiable, noted that no reporting received to date to indicate non-compliance.
48	UNVERIFIED	Full compliance could not be verified
49	N/A	No research use noted, therefore not applicable.
<b>Regulations relating to disclosure of personal information</b>		
5	COMPLIANT	
6	N/A	No formal examination noted.
8	N/A	No research agreement in place.

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Maturity Rating against Privacy Maturity Model

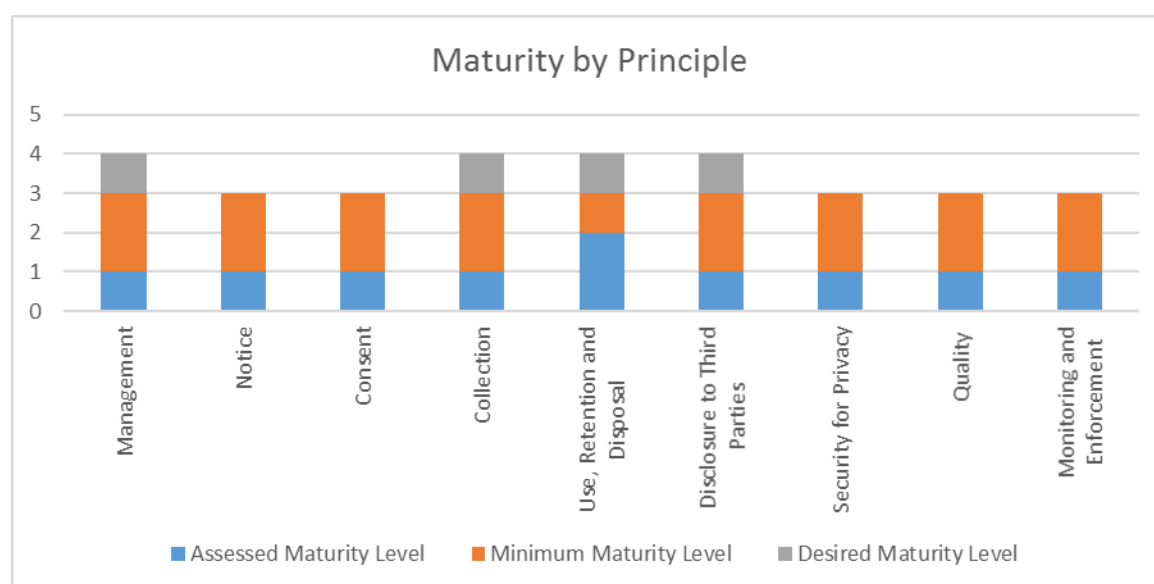
Using the Privacy Maturity Model (**Appendix A refers**), the assessed maturity, minimum maturity and desired maturity are illustrated in the graph below.

**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.

Please note that departments with data which has been assessed as lower risk are only required to reach the minimum maturity level. As MACA does not deal with higher risk data, this department is expected to work towards the minimum maturity level set out below.



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
<b>Management</b> The department defines, documents, communicates and assigns accountability for its privacy policies and procedures	Ad Hoc	<ul style="list-style-type: none"> <li>Privacy policies have not been formally designed and documented.</li> <li>An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.</li> <li>An ATIPP Coordinator has been assigned and has taken the training offered by the Privacy Office.</li> </ul>



# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>The ATIPP Coordinator position is unfunded for this department and as a result the Coordinator is also the records Coordinator, there is a lack of resources required for the maturity to be more than Ad Hoc.</li> </ul> <p><i>See observations 1-3.</i></p>
<p><b>Notice</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms (hard copy and online) used to collect personal information.</li> </ul> <p><i>See observation 4.</i></p>
<p><b>Consent</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent is obtained on some personal information collection forms but not all. Explicit consent is not obtained.</li> </ul> <p><i>See observation 5.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>Methods and forms of collecting information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.</li> <li>A procedure/process does not exist to ensure only information needed is collected.</li> </ul> <p><i>See observations 7-8.</i></p>
<p><b>Use, retention and disposal</b></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>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for.</li> <li>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.</li> </ul> <p><i>See observation 7 &amp; 8.</i></p>

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Disclosure to third parties</b></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>	Ad Hoc	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Information sharing agreements do not exist with other departments to provide instructions or requirements 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.</li> </ul> <p><i>See observation 9.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place. Physical access to personal information is not as restricted with the exception of the office of the fire marshal.</li> <li>• Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>• Tests of safeguards in place are not performed.</li> </ul> <p><i>See observation 10.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Monitoring and enforcement</b></p> <p>The department monitors compliance with its privacy policies and procedures and has procedures to address</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address monitoring and enforcement.</li> <li>• Monitoring and enforcement are not being done at present.</li> </ul>

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
privacy-related complaints and disputes.		See observation 1.

### Observations and Recommendations

#### Observation 1

##### Privacy policy has not been designed and documented

- The responsibility and authority to develop the privacy policies has been unclear.
- The ATIPP Coordinator has limited time and resources to dedicate to ATIPP policies and procedures, specifically in regards to part 2 of the legislation.

#### 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:
MACA supports this recommendation and would work with the Department of Justice to implement their Privacy Policy and Guidelines within the department.	This timeline is beyond MACA's control and is dependent on the Department of Justice

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### 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 identified and 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 adequately protected under ATIPP.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### 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:
MACA will take preliminary steps to consider how to implement a Department-wide inventory of personal information that is collected for all of the program we administer for NWT residents	<ul style="list-style-type: none"><li>• MACA can complete preliminary steps by March 31, 2019.</li><li>• MACA will align subsequent actions with the recommended Department of Justice's Privacy Policy and Guideline, which MACA anticipates would offer some manner of standardization for departmental approaches to such inventories.</li></ul>

### Observation 3

#### There is a lack of resources and experience to support ATIPP within the Department

- ATIPP Coordinator is an unfunded position held by the records Coordinator who previously worked full time in the records role. The ATIPP Coordinator is unable to address the requirements of ATIPP compliance while performing split roles.
- Training provided to the ATIPP Coordinator consisted of a three day course provided by the Access Privacy Office. Currently the knowledge level is inadequate to allow the ATIPP Coordinator to effectively complete their full ATIPP responsibilities.

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Risk Profile:

Risk Impact	Without a set role with assigned accountabilities as outlined in a job description, the privacy function (whether part of another role or in its own capacity) will be limited in ability to fulfill the role's responsibilities. Without additional training options or availability, there is increased risk that the privacy Coordinator may not have the full understanding required to carry out the role.
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 roles and responsibilities of the ATIPP Coordinator be defined, addressing both ATIPP Part 1 and Part 2.
- Training for ATIPP Coordinators be reviewed and adjusted as needed to ensure that there is both awareness and understanding of the full responsibilities for ATIPP compliance. This will allow for better provision of guidance to the department.
- The department should evaluate capacity and capability of current resources. Awareness of resources for ATIPP understanding, training and guidance is required along with support for ATIPP compliance activities.

### Management Response:

Action Plan	Completion Date:
<ul style="list-style-type: none"><li>• The overarching policy developed by the Department of Justice will be useful in clarifying the roles and responsibilities of the Coordinator.</li><li>• MACA will work with the Department of Justice to review and improve the training provided to ATIPP Coordinators</li><li>• MACA will do its own evaluation of the training given to ATIPP Coordinators and the support that the Department of Justice provided to the Department and determine where improvements need to be made.</li></ul>	<ul style="list-style-type: none"><li>• Point 1 completion date will be tied to when the Privacy Policy and Guidelines are developed by Justice</li><li>• For points 2 and 3 – March 31, 2019</li></ul>

### Observation 4

#### **Forms, hard copy and electronic, used to collect personal information are not consistently providing the required notice**

- Notice regarding consent, collection, use, retention and disposal, third party disclosure, security protection, quality and monitoring and enforcement is missing from most forms.
- The department is not compliant with ATIPP Part 2 legislation because of the lack of notice provided specifically related to individuals being informed about how to contact the entity with inquiries, complaints and disputes.

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to provide the required notice to the individuals.

### Management Response:

Action Plan	Completion Date:
MACA will review all of its forms and update them to ensure they comply with ATIPP and the Department of Justice's Privacy Policy and Guidelines.	MACA will align the timing of this work to support and be in compliance with the recommended Department of Justice's Privacy Policy and Guideline.

### Observation 5

#### Not all forms, hard copy and electronic, used to collect personal information require consent from the individual

- Implicit consent is obtained by the individual's signature on the collection form but not all forms require the signature of the individual.
- Explicit consent is not obtained when sensitive information is collected.

### Risk Profile:

Risk Impact	When consent is not obtained there is an increased risk that full disclosure has not been made; which would result in non-compliance with ATIPP
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- All forms, hard copy and electronic, used to collect personal information be reviewed and updated to require the individual's signature or explicit consent if sensitive information is being collected.

### Management Response:

Action Plan	Completion Date:
MACA will review all of its forms and update them to ensure they comply with ATIPP and the	MACA will align the timing of this work to support and be in compliance with the recommended

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

Department of Justice's Privacy Policy and Guidelines.	Department of Justice's Privacy Policy and Guideline.
--	---

### Observation 6

#### Methods of collection are not reviewed by ATIPP Coordinator prior to implementation

- Department develops and uses their own methods of collection of personal information.
- New collection methods are not reviewed by ATIPP Coordinator along with key stakeholders as required to ensure they are fair and lawful.
- New collection methods are not reviewed to ensure only information needed for its purpose is being collected. A privacy impact assessment is not performed.

#### Risk Profile:

Risk Impact	Without a review of collection methods being introduced, there is increased risk of non-compliance with ATIPP legislation during these new collection methods.
Risk Responsibility	Director
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 all new methods of information collection be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized which specifies actions to be taken by the ATIPP Coordinator to validate only information needed is collected through fair and lawful means.
- A privacy impact assessment be performed for all new information collection methods or changes to existing methods.

#### Management Response:

Action Plan	Completion Date:
<ul style="list-style-type: none"> <li>• MACA will develop a work plan to a) review its information collection processes and b) to implement any necessary procedures to ensure that information is being collected by fair and lawful means.</li> <li>• MACA anticipates doing so under the guidance of the department of Justice's Privacy Policy and Guidelines.</li> </ul>	<ul style="list-style-type: none"> <li>• March 31, 2019 (subject to any timelines required to support the rolls out of recommended DOJ policies and guidelines)</li> <li>• MACA will align the timing of any subsequent actions to support and be in compliance with the recommended Department of Justice's Policy and Guidelines</li> </ul>

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Observation 7

#### Procedures do not exist to ensure only information needed is collected

- Existing methods of collection are not reviewed by the ATIPP Coordinator along with key stakeholders as required to ensure only information needed is being collected.

#### Risk Profile:

Risk Impact	If additional information is collected beyond that required by the use for which disclosure was made to the individual, the department will not be in compliance with ATIPP legislation
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

#### Recommendations:

We recommend that:

- The department reevaluate and reassess the current information collection needs to support the department mandate.
- The personal information essential for the collection purpose be clearly documented and distinguished from optional information for each program for which personal information collection is required.
- Existing forms be reviewed against documented personal information essential for use and changed as necessary to collect only the information required for the purpose for which it's being collected.

#### Management Response:

Action Plan	Completion Date:
<ul style="list-style-type: none"><li>MACA will evaluate the information that it collects and the manner it collects it in, to ensure that it is only collecting what it needs to deliver programs.</li><li>Forms are to be reviewed on an annual basis to ensure compliance</li></ul>	MACA will initiate a work plan in 2018-2019 with expected completion of initial analysis by March 2019. Annual review going forward.

### Observation 8

#### Collection of information not directly from the individual is not being disclosed

- A process is not in place to identify situations and inform individuals when the department acquires or develops information about them.

#### Risk Profile:

Risk Impact	When collection of personal information is not disclosed, the department is not in 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



# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Recommendations:

We recommend that:

- Privacy processes be developed to address situations and/or circumstances where information is developed or acquired about individuals and procedures be implemented to ensure individuals are informed.

### Management Response:

Action Plan	Completion Date:
<ul style="list-style-type: none"><li>• MACA will consider where information is being collected about individuals instead of from individuals and, where necessary, create a process to inform them.</li><li>• The ATIPP Coordinator will hold annual ATIPP-Privacy-Collection of Personal Information Sessions for the Department</li></ul>	<ul style="list-style-type: none"><li>• MACA will initiate a work plan in 2018-2019 with expected completion of initial analysis by March 2019. Annual review going forward.</li></ul>

### Observation 9

#### Information sharing agreements do not exist between MACA and other GNWT departments

- A listing does not exist which details the type of information shared through information sharing agreements, with which departments and for what use.

### Risk Profile:

Risk Impact	When information sharing agreements are not in place there is increased risk that proper disclosures are not made to the owners of the personal information being shared.
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 listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from MACA and that the agreements provide instructions or requirements 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.

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

### Management Response:

Action Plan	Completion Date:
MACA supports interdepartmental sharing of information. We agree as part of developing our initial inventory, we will also inventory any information that is being shared with other departments, and as part of this inventory we will determine if an Information Sharing Agreement is required. Where changes to the inventory of information shared between departments changes as part of the annual process, the department will also review the need for information sharing agreements.	As we continue to implement this process beginning in 2018-2019, we will establish processes for the regular review of information sharing across departments, and will review the process and inventory on an annual basis, and make adjustments to the process or inventory annually.

### Observation 10

#### Physical security does not exist for all hard copy records of personal information

- Physical access restrictions do not exist for all hard copy records.
- Not all hard copy records containing personal information are stored in secure and locked cabinets.

### Risk Profile:

Risk Impact	When records are left in locations that can be accessed there is increased risk that personal information will be seen by people who are not part of the use for which the disclosure was made upon collection. This would result in non-compliance with ATIPP legislation.
Risk Responsibility	Director
Risk Mitigation Support	Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office

### Recommendations:

We recommend that:

- A procedure, as supported by policy, be formalized that details how physical records containing personal information be stored to ensure all documents are stored in secure cabinets with restricted access.
- Storage cabinets or other storage equipment be acquired to allow for restricted access and to prevent accidental disclosure due to natural disasters and environmental hazards.

### Management Response:

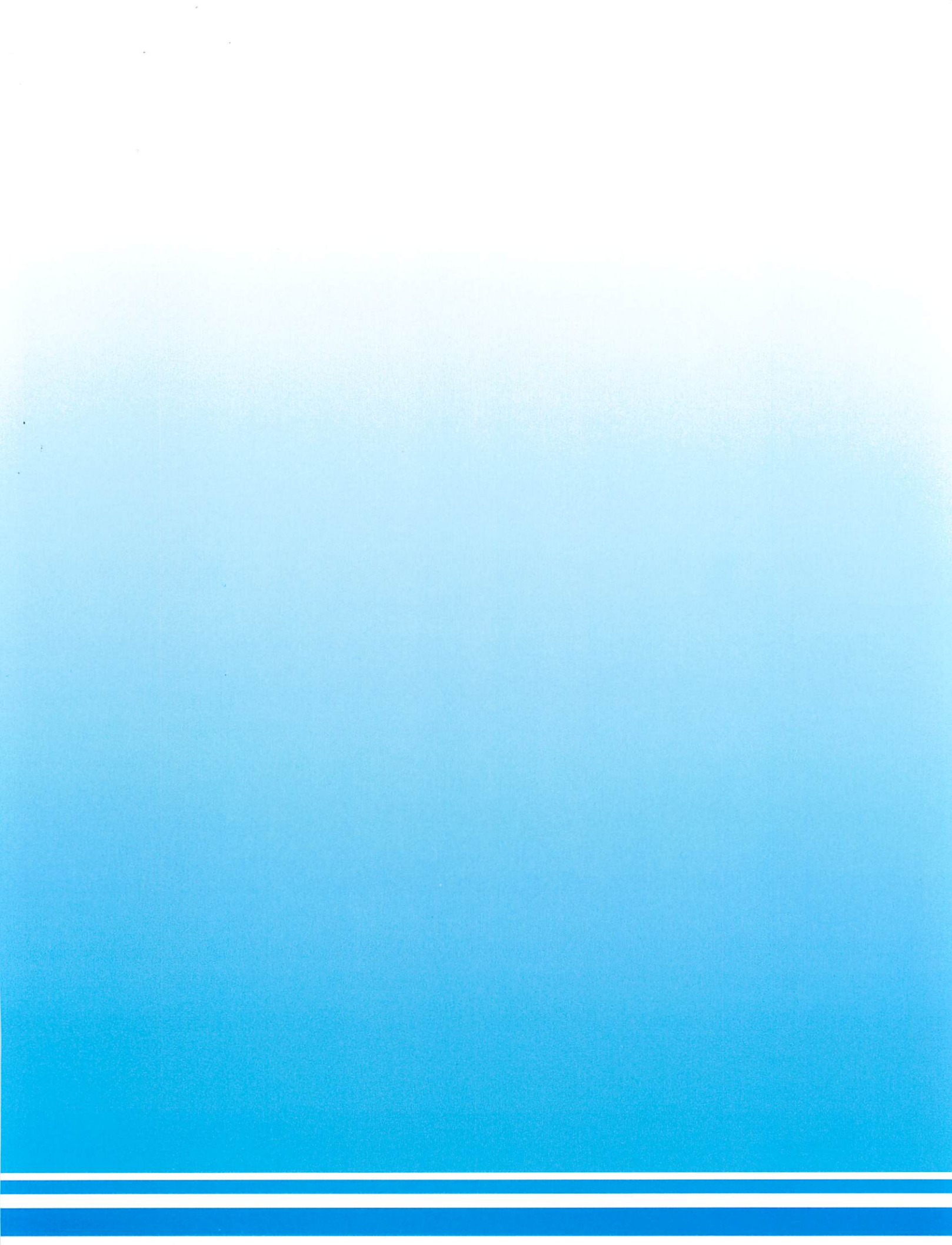
Action Plan	Completion Date:
MACA will lock filing cabinets that contain confidential information to the extent that we have paper files and ensure access controls are in place.	For cabinet securement, a process will be developed May/June 2018, with initiation implemented as soon as possible. For areas where keys/locks are not matched and new

# DEPARTMENT OF MUNICIPAL AND COMMUNITY AFFAIRS

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

	cabinets may need to be ordered, anticipated timeline is October 2018.
--	--

Management responses were received from Sherry Drover via email with copies sent to Terry Kungl, Gary Schauerte, Rose Jiang and Eleanor Young.





MAY 08 2019

File: 7820-20-GNWT-151-135

**CONFIDENTIAL**

MR. MARTIN GOLDNEY  
DEPUTY MINISTER  
JUSTICE

**Audit Report: Revenue Process Audit**  
**Audit Period: As of March 31, 2019**

---

**A. SCOPE AND OBJECTIVES**

The Audit Committee approved an operational audit of Government of Northwest Territories (GNWT) Revenue Process. The examination of the Department of Justice (Justice) internal controls for the revenue process was part of the overall audit project. This report identifies issues specific to the Justice department.

In assessing the revenue process for the GNWT, a number of recommendations affected more than one department. These items were reported in the “*GNWT Revenue Process Report*” and forwarded to the Department of Finance for further action. The Justice report forms part of the “*GNWT Revenue Process Report*.”

**B. BACKGROUND**

The Financial Administration Manual (FAM) provides direction on processing of over \$300 million in GNWT generated revenue. The Justice revenue consisted of:

- Regulatory revenue such as court fees & fines and Public Trustee fees, and
- Program revenue such as inmate recoveries and air charter recoveries.

According to FAM, the roles and responsibility for establishing the fee, the fee rationale, recording, and receipt of money were allocated to departments, Department of Finance (Finance) Financial Reporting/Collection Services, Management Board Secretariat, and the Comptroller General (**Appendix A refers**).

.../2

Specific phases of GNWT revenues processing were assigned to the departments and the following sections in Finance: System for Accountability and Management, Financial Employee Shared Services (FESS), Financial Reporting/Collection Services, Management Board Secretariat, and the Comptroller General (**Appendix B refers**).

We engaged the services of Crowe MacKay LLP through a competitive Request for Proposal process to conduct the audit.

**C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS**

The audit report, “*Department of Justice, Revenue Process Audit Report*,” made a number of observations and recommendations specific to Justice (**Schedule I refers**).

In assessing Justice’s revenue processes, the contractor determined that there was:

- Compliance with FAM 620 (collection of receivables) and 620.01 (collection of accounts receivables)
- Non-compliance with FAM 610.01 (rationale for fees charged)

The contractor was unable to find sufficient documentary evidence to make an assessment regarding FAM 605 (recording revenue) and FAM 610 (establishment of fees).

In examining the internal control capacity for the six revenue processes, the contractor assessed that requirements were met in two areas and there was a gap in four areas.

Justice Revenue Process Area	Internal Control Capacity Level	
	Current	Required
Role definition and responsibility	3	3
Rate setting and review	2	3
Budget setting	2	3
Invoicing	2	3
Accounts receivable review / collection	2	3
Monitoring	3	3

An internal control capacity at a defined level (rating of 3) was adequate to meet the needs of Justice. A detailed risk assessment of revenue processes could identify a need for a more mature internal control capacity in specific areas.

The contractor made nine observations with associated recommendations. The common theme in these recommendations was the need to document the revenue policy and processes. The management responses to the recommendations have been incorporated in the attached report.

Similar recommendations were made by the contractor in reviewing the four departments. Justice may wish to co-ordinate with the Office of the Comptroller General and the Director of Finance & Administration Committee in addressing the common issues.

Our scheduled audit process will begin in about six months to assess the management action plans in addressing the risks.

#### **D. ACKNOWLEDGEMENT**

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



T. Bob Shahi  
Director, Internal Audit Bureau  
Finance

Attachments

## DEPARTMENT OF JUSTICE

### SCOPE AND OBJECTIVES

The Internal Audit Bureau issued a request for proposal for an operational audit reviewing the Revenue Process for the Government of the Northwest Territories (GNWT) generated revenue approved by the Audit Committee for 2018-2019 Audit Work Plan. Crowe MacKay LLP (Crowe) was the successful proponent.

Focus for this audit consisted of evaluating internal controls designed and implemented regarding revenue and in alignment with the FAA and FAM. Crowe specifically looked at the controls designed and implemented at Financial and Employee Shared Services (FESS) as well as within 4 departments chosen for sample testing (Justice; Education, Culture and Employment; Environment and Natural Resources; Infrastructure). The scope excluded the NWT Housing Corporation, GNWT departments not selected for testing as denoted above, and the 9 public agencies. Audit work focused directly on high-level policies and procedures as well as control frameworks and control processes. Crowe's evaluation did not include transaction-level revenue testing for this audit.

Testing of the 4 selected departments consisted of reviewing the main revenue functions/processes which have been assigned, and are the responsibility of, each department. These responsibilities are outlined as follows:

1. Role definition and responsibilities;
2. Training;
3. Rate setting and review;
4. Budget setting;
5. Invoicing;
6. Accounts Receivable/Collection Management; and
7. Monitoring Processes (i.e. budget vs. actual comparison; pertinent reconciliations).

We reviewed key controls related to each of the areas noted above, taking into account the maturity of controls designed and implemented to manage revenue processes. This testing was conducted on current approaches to, and compliance activities of, each department.

### DEPARTMENTAL BACKGROUND

The Department of Justice (Justice) meets its responsibilities through the following functions:

- Services to Government;
- Policing Services;
- Services to the Public;
- Office of the Regulator of Oil and Gas Operations;
- Corrections;
- Community Justice and Policing;
- Court Services, and;
- Legal Aid Services.

General revenues generated by Justice consist of the following:

- Regulatory Revenues – Access to Information and Protection of Privacy Fees, Court Fees & Fines, Land Title & Legal Registries Fees, Maintenance Enforcement Program Attachment Costs, Public Trustee Fees, Rental Office Fees and Operators Licenses;
- Program Revenues – Air Charter Recoveries, Young Offenders Special Allowance Nunavut Exchanges of Services, Community Parole, Federal Exchange of Services, Legal Aid



Requirements, Contract Management Committee Provincial Territorial Secretariat, Inmate Recoveries.

The revenue function consists of the following areas of responsibility within the department:

- Access to Information and Protection of Privacy Fees is the responsibility of Access and Privacy Office and Corporate Services.
- Court Fees & Fines are the responsibility of court clerks, the administrative court officer and Sheriff Finance Officer.
- Land Title & Legal Registries Fees is the responsibility of the finance and administration assistant in Legal Registries.
- Maintenance Enforcement Program Attachment Costs is the responsibility of the Maintenance Enforcement Program Manager.
- Public Trustee Fees are the responsibility of the Public Trustee Office senior finance clerk.
- Rental Office Fees are the responsibility of the rental office administrator and FESS.
- Air Charter Recoveries are the responsibility of the financial operations specialist in corporate services and Administrative Court Officer.
- Young Offenders Special Allowance Nunavut Exchanges of Services is the responsibility of Corporate services.
- Community Parole is the responsibility of Corrections Administration.
- Federal Exchange of Services is the responsibility of Corrections Administration.
- Legal Aid Requirements is the responsibility of senior finance officer, Legal Aid Commission.
- Contract Management Committee Provincial Territorial Secretariat is the responsibility of assistant director, corporate services.
- Inmate Recoveries is the responsibility of manager, administrative and support services and/or facility admin officers.

The department interacts with various service areas of the GNWT Department of Finance in order to fully address all revenue processes, such as: i) Financial and Employee Shared Services; ii) Management Board Secretariat; and iii) Financial Reporting and Collections.

## METHODOLOGY

Justice has varied services with revenues managed by staff in different areas. As a result, it was determined that for this department, interviews would be conducted with the Director, Corporate Services, as well as with the people who were responsible for compliance in each area of the revenue processes. From these interviews, an overall assessment of the maturity level of the department, in relation to each main revenue function, was made.

## OVERVIEW

### Compliance with FAA and FAM

The Financial Administration Manual (FAM) has been prepared in such a manner as to ensure that the requirements of the Financial Administration Act (FAA) have been met. Crowe has therefore made an assessment of the overall compliance of the department with the FAM in relation to sections within the scope of this audit.

The table below has the assessment of compliance, and if relevant, an explanation for why the department is not compliant. There may be areas within a program where partial compliance is in place, but for the purposes of this table, the department has been rated as compliant, partially compliant, non-compliant, or unverifiable.

Based on the audit work performed, as well as the inability of the Justice department to provide the evidence necessary to conclude on internal control effectiveness, Crowe has concluded that additional

work is required by Justice to design and implement internal controls to sustain an audit opinion of “Compliant”. This will include the necessary documentation required to support that key controls are operating effectively. Support for this assessment is provided in the following table:

Section Policy	Compliance Assessment	Reason for Non-Compliance
<b>605 – Recording Revenue</b>		
Revenue earned for work performed, goods supplied, services rendered, or amounts entitled in the fiscal year must be recorded in accordance with approved systems and procedures in a timely manner.	<b>Unverifiable</b>	Unable to verify if revenue earned is recorded in accordance with approved systems and procedures because not all significant approved systems and procedures are documented.
<b>610 – Establishment of Fees</b>		
Where economically and administratively feasible, GNWT Departments and Public Agencies shall charge fees for licenses, permits and services rendered to the public. The authorized rates for any fee shall bear a reasonable relationship to the cost of administering the license or service or be authorized at a rate lower than full cost recovery, where appropriate.	<b>Unverifiable</b>	Regulated rates are reviewed every five year as per FMB direction. The rationale for rate changes or unchanged rates at the five year review for other than inflationary changes are not documented as such it is not verifiable whether the rates address current costs of the related services or license.
<p><b>IB610.01 Rationale for Fees Charged</b></p> <p>GNWT Departments and Public Agencies are to ensure that fees are collected, safeguarded, and accounted for.</p> <p>A rationale for each fee charged must be kept available for audit purposes.</p> <p>The rationale in support of each fee charged must include:</p> <ul style="list-style-type: none"> <li>- pricing details;</li> <li>- the price/rate basis, including direct, indirect, and accounting and system costs; and,</li> <li>- the time period for cyclical fee reviews.</li> </ul> <p>In the case of a regulatory service, a fee or charge fixed on a total cost recovery basis may not be warranted. The fee for such a service may be collected from the ultimate user or from an intermediary who considers the expense a cost of doing business.</p>	<b>Non-Compliant</b>	The rationale for rate changes or unchanged rates other than inflationary changes at the five year review are not documented.
<b>620 – Collection of Receivables</b>		
GNWT Departments and Public Agencies are responsible to	<b>Compliant</b>	AR reviewed and

Section Policy	Compliance Assessment	Reason for Non-Compliance
<p>collect all accounts receivable promptly, efficiently, and in a thoroughly accountable manner, unless otherwise directed by the Comptroller General or their delegate.</p>		<p>actioned monthly</p> <p>Follow-up occurs on balances outstanding between 30 and 90 days.</p> <p>“On Account” balances in the department’s AR are reviewed monthly as part of the AR.</p> <p>“On Account” balances at December 30, 2018 amounted to less than \$500.</p> <p>Monthly checklist is used for corporate service finance staff to ensure monthly and quarterly billings are prepared, accounts receivable are reviewed and variances are completed.</p> <p>The department understands the role and responsibility of the Collections unit.</p>
<p><b>IB 620.01 Collection of Accounts Receivable</b></p> <p>Except as described below, an invoice must be prepared, recorded, and delivered to the debtor as soon as a receivable is created and the debtor must be given 30 calendar days from the date of the invoice to return payment to the GNWT or Public Agency.</p> <p>If payment is not received within 30 days of the date of the invoice, the responsible department or Public Agency shall attempt to collect by notifying the debtor in writing that payment is overdue and payable immediately. At this point, the debt has become an overdue receivable.</p> <p>If payment is not received during the next 30 days (i.e., within 60 days of the date of the invoice) the responsible department or Public Agency shall attempt to collect again by notifying the debtor by telephone and in writing that payment is now 30 days overdue and payable immediately.</p> <p>If payment is not received during the next 30 days (i.e., within 90 days of the date of the invoice) the overdue receivable becomes a delinquent account receivable. The responsible department or Public Agency shall:</p> <p>attempt to collect again by notifying the debtor that payment</p>	<p><b>Compliant</b></p>	<p>Revenues on account are invoiced and the debtor is provided 30 days from the date of invoice to make payment.</p> <p>FESS sends customer statements for all accounts receivable outstanding 30 days.</p> <p>The department reviews accounts receivable outstanding 30-90 days and makes collection efforts within the department by making phone calls to the customers.</p> <p>The collection responsibility is assigned correctly to the collections department</p>

Section Policy	Compliance Assessment	Reason for Non-Compliance
is now 60 days overdue and payable immediately; and transfer collection responsibility to the Financial Reporting and Collections Section, Finance, immediately.		at 90 days.

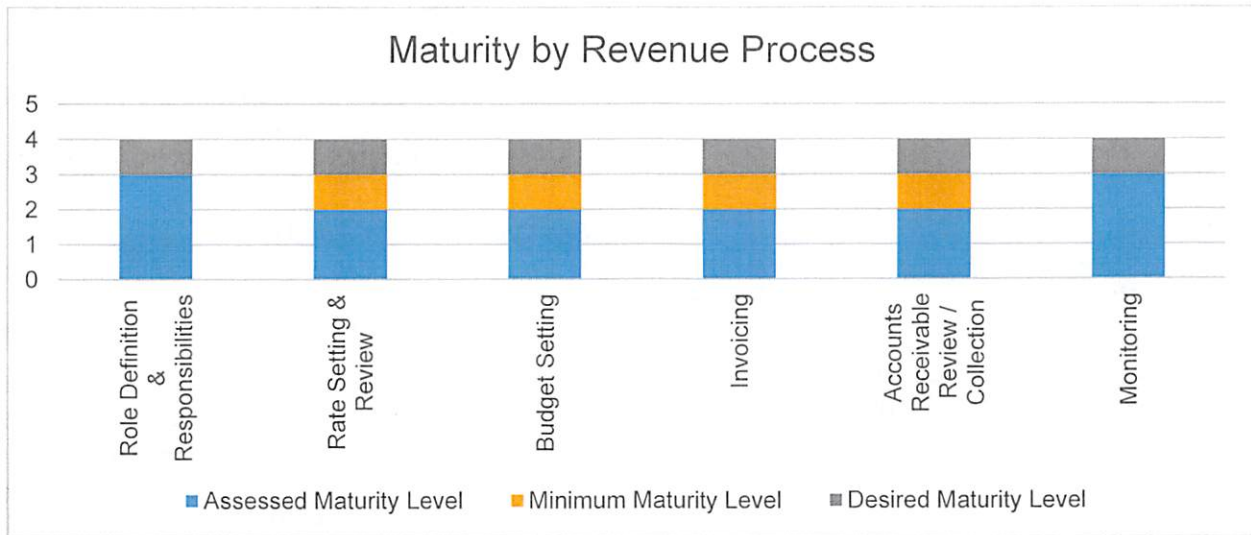
**Maturity Rating Considering GNWT Internal Control Capacity Model**

Using the GNWT Internal Control Capacity Model (**Appendix C**), 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. Desired maturity level has been set by Crowe at a level that is considered achievable over time by the department and taking into account the level of risk in the department.



Overall findings, including rating of the department against each revenue process area, is summarized in the following table:

Revenue Process Area	Assessed Maturity Level	Findings and Comments
<p><b>Role Definition and Responsibilities</b></p> <p>The department defines, documents, communicates and assigns accountability for its revenue processes and procedures. Roles are defined and responsibilities address all</p>	Defined	<ul style="list-style-type: none"> <li>Job descriptions exist for the positions outlined above under departmental background as responsible for the department's general revenue functions.</li> <li>Job descriptions include responsibilities related to specific general revenue cycle</li> </ul>

Revenue Process Area	Assessed Maturity Level	Findings and Comments
aspects of revenue.		<p>components.</p> <ul style="list-style-type: none"> <li>Job descriptions reviewed by Crowe have not all been updated within the last four years.</li> </ul> <p><i>See Observation 1.</i></p>
<p><b>Rate Setting &amp; Review</b></p> <p>The department reviews rates on a set periodic basis to ensure rates are current and new revenue sources have been considered.</p>	Repeatable	<ul style="list-style-type: none"> <li>Regulated rates and fees are charged in accordance with the regulation and are reviewed every five years per FMB direction.</li> <li>Regulated rates history is tracked by the department which details the review period and inflationary increases.</li> <li>Rationale and process for non-inflationary rate changes is not documented.</li> <li>Non-regulated rates and fees are reviewed every 5 years for inflation purposes and against fees charged by other jurisdictions. This process is not documented.</li> <li>New sources of revenue are considered when new programs or initiatives are planned but a formal process does not exist.</li> </ul> <p><i>See Observation 2, 3 and 4.</i></p>
<p><b>Budget Setting</b></p> <p>The department clearly defines and documents the revenues expected for each year with explanations for any material changes from prior years.</p>	Repeatable	<ul style="list-style-type: none"> <li>Assistant Director, Corporate Services prepares the operating budget with revenue estimates. Clarity on roles and responsibilities of Assistant Director, Corporate Services exists.</li> <li>Budget of revenues is based on prior year estimates and actuals unless rate changes have been approved and then the budget is adjusted to reflect the fee increases.</li> <li>Process for review of revenue budget assumptions and rationale for estimates are not documented.</li> </ul> <p><i>See Observation 5.</i></p>
<p><b>Invoicing</b></p> <p>The department ensures that invoices are prepared in a timely manner, and are accurate and complete.</p>	Repeatable	<ul style="list-style-type: none"> <li>Invoices are not issued for the majority of the department's revenue streams because payment is received at the time of service.</li> <li>Processes are in place to record revenues received in cash or by online payment at the time the service is provided.</li> <li>Processes are in place to ensure all revenues earned are recorded as revenues</li> </ul>

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<p>for revenues received by cheque or direct payment.</p> <ul style="list-style-type: none"> <li>• Monthly checklist is used for corporate service finance staff to ensure monthly and quarterly billings are prepared, accounts receivable are reviewed and variances are completed.</li> <li>• Processes are documented for some of the significant regulatory revenue streams but are not documented for all significant revenue streams.</li> </ul> <p><i>See Observation 6.</i></p>
<p><b>Accounts Receivable Review / Collection</b></p> <p>The department monitors receivables on a set periodic basis and ensures that follow-up takes place if revenues are not received as expected.</p>	<p>Repeatable</p>	<ul style="list-style-type: none"> <li>• The department has a "Finance General" email established for emails from FESS and a department representative has been assigned.</li> <li>• The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque.</li> <li>• The number of receipts by cheque by the department are insignificant; the majority are received by direct payment.</li> <li>• The department's process for addressing emails received from FESS is not documented.</li> <li>• The process the department has for addressing emails received from FESS regarding unallocated receipts by cheque does not include specific procedures to be taken by department staff.</li> <li>• The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting.</li> <li>• The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting.</li> <li>• The procedures to be taken when an unclaimed deposits email is received from Department of Finance - Financial Reporting have not been established and documented.</li> <li>• Accounts receivable are reviewed monthly and actions are taken within department to follow-up on balances outstanding between 30 and 90 days.</li> </ul>

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>The accounts receivable review is a documented policy by the department.</li> <li>“On Account” balances in the department’s accounts receivable are reviewed monthly as part of the monthly accounts receivable review.</li> <li>“On Account” balances at December 30, 2018 amounted to less than \$500.</li> <li>Monthly checklist is used for corporate service finance staff to ensure monthly and quarterly billings are prepared, accounts receivable are reviewed and variances are completed.</li> <li>The department understands the role and responsibility of the Collections unit.</li> </ul> <p><i>See Observations 7, 8 and 9.</i></p>
<p><b>Monitoring</b></p> <p>The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are not being received as expected.</p>	Defined	<ul style="list-style-type: none"> <li>Monthly and quarterly variances are prepared by Budget Analyst based on budgeted revenues versus actuals revenues per reports from SAM.</li> <li>Monthly checklist is used for corporate service finance staff to ensure monthly and quarterly billings are prepared, accounts receivable are reviewed and variances are completed.</li> <li>Explanations for variances are documented.</li> <li>Variance reports are reviewed and provided to Management Board Secretariat.</li> <li>Process for variance analysis is documented.</li> </ul>

## OBSERVATIONS AND RECOMMENDATIONS

### Observation 1

**Job descriptions have not been updated within the last four years.**

- Although the department has job descriptions for all roles in the revenue cycle that include revenue related duties and responsibilities, some job descriptions have not been updated within the last 4 years.

#### Risk Profile:

Risk Impact	Without updated job descriptions, duties, responsibilities and assignment changes may not be reflected in the job descriptions and job descriptions will not be readily available for the hiring process
-------------	--

	should a position become vacant; possibly increasing the time the position is vacant.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

**Recommendations:**

We recommend that:

- a) Job descriptions should be reviewed every 3-4 years to ensure they accurately reflect the duties and responsibilities of the position.

**Management Response:**

Action Plan	Completion Date:
a) Management accepts this recommendation. Corporate Services job descriptions are reviewed annually in April as part of the performance process. If updates are required, revisions will be provided to job evaluation.	April 30, 2019

**Observation 2**

**Policy and process have not been documented for regulated rates and fees and for non-regulated rates.**

- Although regulated rates and fees are reviewed every five years per FMB direction documentation of fee review is lacking and rationale for fee changes is not documented.
- Non-regulated rates are also reviewed every 5 years for inflation and against other jurisdictions for comparative purposes; this process is not documented.

**Risk Profile:**

Risk Impact	Without clearly documented processes for review of both regulated and non-regulated fees, and review of the legislation for the regulated rates, fees may not be adequate to cover related costs.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

**Recommendations:**

We recommend that:

- a) For each revenue stream, the process established to review rates and fees should be evaluated to ensure the activities required occur on a set periodic basis that adequately addresses economical changes which would impact the rate and fee; the process should be documented including roles and responsibilities.
- b) For regulated rates, documented processes should include a review of legislation to ensure that it is current and supports a fee structure that allows for adequate coverage of related costs.

**Management Response:**

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop procedures for documenting economical changes to inform fee development	April 1, 2020



b) Management accepts this recommendation. Develop directives with respect to 5 year review of fees and associated legislation.	April 1, 2020
---	---------------

### Observation 3

#### Rationale for fees charged is not documented and available for review as required by the FAM.

- Although staff members were able to explain rates and processes involved around setting and reviewing rates (subject to Observation 1 above), there was not a documented rationale available for review as required by IB610.01 of the FAM.

#### Risk Profile:

Risk Impact	Without clearly documented rationale for rates in place, there is increased risk that the reason for the type and amount of rates being charged for various services may be incorrect or outdated.
Risk Responsibility	Director, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

#### Recommendations:

We recommend that:

- For each revenue stream, the rationale for the rate should be defined and documented; these should then be kept on hand for review.

#### Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Consolidate and document rationale for rates determined by Justice.	April 1, 2020

### Observation 4

#### A policy has not been designed and documented for assessing new revenue sources.

- The department assesses potential new revenue sources when planning new programs and initiatives as considered by the program manager/lead. However, a documented process does not exist to substantiate the procedures to be followed, or evidence to be maintained, to validate the steps taken.

#### Risk Profile:

Risk Impact	Without a clearly defined and documented policy for assessing new revenue sources on a periodic basis, there is an increased risk that fees will not be established to assist with cost recovery of the program/service, or the fees will not be set at appropriate rates.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

#### Recommendations:

We recommend that:

- A policy should be formalized that requires revenues to be considered for all new programs or initiatives at the planning stage, including maintenance of records to substantiate decisions made.

**Management Response:**

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop directives for assessing new revenue sources. Share directive with program management.	June 30, 2019

**Observation 5**

**Procedures for review of assumptions used in budget preparation are not fully documented.**

- General revenues of the department are very consistent from year-to-year, or are insignificant in size.
- Procedures for review of budgeted revenues for rate changes and/or other impactful factors are not documented.

**Risk Profile:**

Risk Impact	A lack of documentation and review of the assumptions used in budget preparation, and lack of documentation for the process used to ensure rate changes and other impacts have been taken into account, can increase the risk of inaccurate budgeting.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

**Recommendations:**

We recommend that:

- Procedures used to ensure that budgeted revenues are based on clearly thought out assumptions, reviewed for the impact of rate changes, or impacts to rates, should be documented and followed going forward.

**Management Response:**

Action Plan	Completion Date:
a) Management accepts this recommendation. Document procedures for development of revenue budgets.	June 30, 2019

**Observation 6**

**Revenue processes are not fully documented.**

- Processes are in place for each significant revenue stream to ensure revenues earned are recorded, but are only documented for regulatory revenues; processes for significant program revenues are not documented.

**Risk Profile:**

Risk Impact	Without documented program revenue policies and procedures, consistent direction cannot be given to departmental personnel and consistent application may not occur, which could result in earned revenues not being recorded and receipts not being collected.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

### Recommendations:

We recommend that:

- a) Revenue policies and processes in place should be fully documented for significant program revenue stream and should include roles and responsibilities, how revenues are initiated, and the controls in place to ensure all revenues earned are recorded.

### Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop procedures for ensuring each major program revenue stream is accounted for.	June 30, 2019

### Observation 7

**Process for addressing unallocated cheque emails from FESS is not documented and the process lacks procedures to be performed.**

- The department representative, Assistant Director, Corporate Services, for the "Finance General" email account forwards emails received from FESS for unallocated cheques to the applicable department staff for review. FESS sends an email when a cheque has been received that cannot be allocated and the department is given 48 hours to reply.
- If the cheque is identified by department staff as being for Justice, and the purpose of the receipt is known, the department staff will email the department representative and the department representative will email FESS with instructions on how to apply the receipt.
- The process is not documented and specific procedures to be taken by department staff upon receipt of an email for an unallocated cheque from the department representative have not been designed and documented.

### Risk Profile:

Risk Impact	Without specific procedures being designed and documented, it may be unclear to staff what should be done when an unallocated cheque email is received, which could result in no action being taken or insufficient action taken. This increases the risk of lost revenue to the department or incorrectly recorded receipts "On Account" to the department. Without a documented process, consistent direction cannot be given to departmental staff, and verbally communicated processes may not be transferred to new staff.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

### Recommendations:

We recommend that:

- a) Procedures should be designed to ensure all possible actions are taken by department staff for unallocated cheques received by FESS.
- b) Processes and procedures should be documented regarding the receipt of unallocated cheque emails from FESS.

### Management Response:

Action Plan	Completion Date:

a) Management accepts this recommendation. Develop written procedures for how staff will action unallocated cheques received from FESS.	April 30, 2019
b) Management accepts this recommendations. Document processes in place for addressing the receipt of the emails from FESS relating to unallocated cheques.	

### Observation 8

#### Processes for direct payment notifications received by department staff are not documented.

- When a direct payment notification is received by department staff the notification is to be forwarded to Department of Finance – Financial Reporting with details of how the payment should be applied.
- The process is not documented and the information to be sent to Financial Reporting with the direct payment notification has not been clearly defined.

#### Risk Profile:

Risk Impact	Without a documented process, consistent direction cannot be given to departmental staff, and verbally communicated processes may not be transferred to new staff. Inconsistent application of the process increases the risk that Justice revenues will be unrecorded.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

#### Recommendations:

We recommend that:

- A process for handling direct payment notifications received by department staff should be documented and should identify the information to be provided to Financial Reporting in addition to the direct payment notification.

#### Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop written procedures for direct payment notifications.	April 30, 2019

### Observation 9

#### Process for addressing unclaimed deposit emails from Financial Reporting is not documented and the process lacks procedures to be performed.

- The Corporate Finance Officer and Assistant Director, Corporate Services, receive all emails from Financial Reporting for unclaimed deposits (direct payments received for which the purpose has not been determined by Financial Reporting).
- The email received is forwarded by Assistant Director, Corporate Services, or Corporate Finance Officer to the applicable department staff for review.
- If a payment is identified by department staff as being for Justice, and the purpose of the receipt is known, the department staff will email the Assistant Director, Corporate Services, with the coding.
- The Assistant Director, Corporate Services, provides the information received to Financial Reporting with instructions on how to apply the receipt.

- The process is not documented and specific procedures to be taken by department staff upon receipt of the unclaimed deposits email have not been designed and documented.

**Risk Profile:**

Risk Impact	Without specific procedures being designed and documented, it may be unclear to staff what should be done when an unclaimed deposit email is received, which could result in no action being taken or insufficient action taken, which could cause lost revenue to the department. Without a documented process, consistent direction cannot be given to departmental staff, and verbally communicated processes may not be transferred to new staff.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

**Recommendations:**

We recommend that:

- Procedures should be designed to ensure all possible actions are taken by department staff for unclaimed deposits identified by Financial Reporting, and ensure the actions taken are timely.
- Processes and procedures should be documented to address unclaimed deposit emails from Financial Reporting.

**Management Response:**

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop written procedures with respect to management of unclaimed deposit emails from Financial Reporting.	April 30, 2019
b) Management accepts this recommendation. Develop written procedures to address emails from Financial Reporting in relation to unclaimed deposits	April 30, 2019

GNWT Revenue Process Audit  
Roles & Responsibilities

**Appendix A**

**Financial Administration Manual**

	Department	Financial Reporting / Collections	MBS / FMB	Comptroller General
<b>Establishment of Fees</b>	<ul style="list-style-type: none"> <li>Deputy Head responsible to set fees and charge for licenses, permits and services rendered to the public</li> <li>Minister responsible to advise the FMB of the introduction, change or removal of a fee within 60 days</li> </ul>	-	MBS may issue directives respecting financial management or administration of a Public Agency	<ul style="list-style-type: none"> <li>May approve Interpretation Bulletins associated with this policy</li> <li>Establish and maintain systems and procedures to ensure the integrity of GNWT financial records and accounting systems</li> <li>Establish/maintain systems and procedures to ensure public money is collected and accounted for, internal controls are in place</li> </ul>
<b>Rationale for Fees Charged</b>	<ul style="list-style-type: none"> <li>Ensure fees are collected, safeguarded, and accounted for</li> <li>Rationale for each fee must be kept for audit purposes</li> </ul>	-	-	
<b>Recording Revenue</b>	<ul style="list-style-type: none"> <li>Deputy Head of dept. responsible to ensure revenues accurately recorded in a timely manner in accordance with GAAP</li> </ul>	-	-	
<b>Receipt of money</b>	<ul style="list-style-type: none"> <li>Responsible for collection and management of all A/R</li> </ul>	Engage courts or outside collection agency	-	

GNWT Revenue Process Audit  
Roles & Responsibilities


**Appendix B**

**Shared Services Agreement**

	Department	FESS	Financial Reporting / Collections	MBS / FMB	SAM Team	Comptroller General
<b>Estimates (Budgets)</b>	• Prepare	-	-	• MBS review/ FMB approval	• Support	<ul style="list-style-type: none"> <li>• Appointed by Minister of Finance</li> <li>• Maintain systems and procedures with respect to the integrity of government financial records and accounting systems</li> <li>• Ensure compliance by GNWT departments, Public Agencies and other reporting bodies with accounting policies and practices</li> <li>• Manage Consolidated Revenue Fund and Public Accounts.</li> </ul>
<b>Variance reports</b>	• Prepare	-	-	• MBS review/ quarterly to FMB	• Support	
<b>Invoices</b>	• Request/ set up	• Acct. approval	-	-	• Maint.	
<b>Cash Payment</b>	• Process in-dept. receipts	• Process all other receipts	-	-	• System support	
<b>Cheque Payment</b>	• Provide coding	• Process/ post	-	-	• System support	
<b>EFT Payment</b>	• Provide invoice/ coding	• Post	• Process	-	• System support	
<b>A/R Mgmt</b>	• Follow-up <90 days; monitoring ongoing	• Stmt. sent to customer	• Follow-up >90 days; external collections; court	-	• System support	
<b>Training</b>	• Dept. training	• FESS training	• FR/ collection training	• MBS training	• SAM-based training	

Acronyms used in the charts below and further into the report are as follows:

Financial Employees Shared Services	FESS
Financial Management Board:	FMB
Management Board Secretariat:	MBS
System for Accountability and Management	SAM

	Effective Date: June 24, 2014	Section Title: Policy Framework and Standards	Section Number: 100
	Chapter Title: Internal Control and Risk Framework		Chapter Number: 150
	Task Title: Internal Control Capacity Model		Task Number: 153

Deliverable	Description
0 - Non-existent	<ul style="list-style-type: none"> <li>The organization lacks procedures to monitor the effectiveness of internal controls.</li> <li>Management internal control reporting methods are absent.</li> <li>There is a general unawareness of internal control assurance.</li> <li>Management and employees have an overall lack of awareness of internal controls.</li> </ul>
1 - Initial/Ad Hoc - Unreliable	<p>Unpredictable environment for which controls have not been designed or implemented.</p> <ul style="list-style-type: none"> <li>Controls are fragmented and ad hoc.</li> <li>Controls are generally managed in silos and reactive.</li> <li>Lack of formal policies and procedures.</li> <li>Dependent on the “heroics” of individuals to get things done.</li> <li>Higher potential for errors and higher costs due to inefficiencies.</li> <li>Controls are not sustainable.</li> <li>Individual expertise in assessing internal control adequacy is applied on an ad hoc basis.</li> <li>Management has not formally assigned responsibility for monitoring the effectiveness of internal controls.</li> </ul>
2 - Repeatable - Informal	<p>Controls are present but inadequately documented and largely dependent on manual intervention. There are no formal communications or training programs related to the controls.</p> <ul style="list-style-type: none"> <li>Controls are established with some policy structure.</li> <li>Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan.</li> <li>Formal process documentation is still lacking.</li> <li>Some clarity on roles and responsibilities, but not on accountability.</li> <li>Increased discipline and guidelines support repeatability.</li> <li>High reliance on existing personnel creates exposure to change.</li> <li>Internal control assessment is dependent on the skill sets of key individuals.</li> </ul>
3 - Defined - Standardized	<p>Controls are in place and documented, and employees have received formal communications about them. Undetected deviations from controls may occur.</p> <ul style="list-style-type: none"> <li>Controls are well-defined and documented, thus there is consistency even in times of change.</li> <li>Overall control awareness exists.</li> <li>Policies and procedures are developed for assessing and reporting on internal control monitoring activities.</li> <li>A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers.</li> <li>Control gaps are detected and remediated timely.</li> <li>Performance monitoring is informal, placing great reliance on the diligence of people and independent audits</li> </ul>



Deliverable	Description
	<ul style="list-style-type: none"> <li>• Management supports and institutes internal control monitoring.</li> <li>• An education and training program for internal control monitoring is defined.</li> <li>• Tools are being utilized but are not necessarily integrated into all processes.</li> </ul>
4 - Managed - Monitored	<p>Standardized controls are in place and undergo periodic testing to evaluate their design and operation; test results are communicated to management. Limited use of automated tools may support controls.</p> <ul style="list-style-type: none"> <li>• Key Performance Indicators (KPIs) and monitoring techniques are employed to measure success.</li> <li>• Greater reliance on prevention versus detection controls.</li> <li>• Strong self-assessment of operating effectiveness by process owners.</li> <li>• Chain of accountability exists and is well-understood.</li> <li>• Management implements a framework for internal control monitoring.</li> <li>• A formal internal control function is established, with specialized and certified professionals utilizing a formal control framework endorsed by senior management.</li> <li>• Skilled staff members are routinely participating in internal control assessments.</li> <li>• A metrics knowledge base for historical information on internal control monitoring is established.</li> <li>• Peer reviews for internal control monitoring are established.</li> <li>• Tools are implemented to standardize assessments and automatically detect control exceptions.</li> </ul>
5 - Optimized	<p>An integrated internal controls framework with real-time monitoring by management is in place to implement continuous improvement. Automated processes and tools support the controls and enable the organization to quickly change the controls as necessary.</p> <ul style="list-style-type: none"> <li>• Controls are considered “word class”, based on benchmarking and continuous improvement.</li> <li>• The control infrastructure is highly automated and self-updating, thus creating a competitive advantage.</li> <li>• Extensive use of real-time monitoring and executive dashboards.</li> <li>• Management establishes an organization wide continuous improvement program that takes into account lessons learned and industry good practices for internal control monitoring.</li> <li>• The organization uses integrated and updated tools, where appropriate, that allow effective assessment of critical controls and rapid detection of control monitoring incidents.</li> <li>• Benchmarking against industry standards and good practices is formalized.</li> </ul>

