



MAY 09 2018

**CONFIDENTIAL**

File: 7820-20-GNWT-151-131

MR. TOM JENSEN  
DEPUTY MINISTER  
INDUSTRY, TOURISM AND INVESTMENT

**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. Julie Mujcin, Director, Finance and Administration, ITI



# INDUSTRY, TOURISM AND INVESTMENT

## Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



## **INDUSTRY, TOURISM AND INVESTMENT**

### **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 9, 2018

File: 7820-20-GNWT-151-131

MR. TOM JENSEN  
DEPUTY MINISTER  
INDUSTRY INVESTMENT & TOURISM

**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 Industry Investment & Tourism was part of the GNWT wide audit project. This report identifies issues specific to your department.

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

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

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

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

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

Overall, the privacy risk for your department was assessed to be “medium” requiring internal control capacity at “defined” 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 process. The immediate task for the department was to document the privacy processes (defined level). Although not necessary from the assessed risk perspective, the department could identify and address privacy exceptions through monitoring (managed level). There was no compelling reason for the department to develop capacity beyond that stage (optimized level) (**Chart I refers**).

Some of the key recommendations made by the contractor were:

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

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

### 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
Privacy Risk Level	Very High					
	High					
	Medium		ITI			
	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 INDUSTRY, TOURISM AND INVESTMENT

### 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 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.

ITI collects personal information through:



**DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT****ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP (PART 2**

- 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

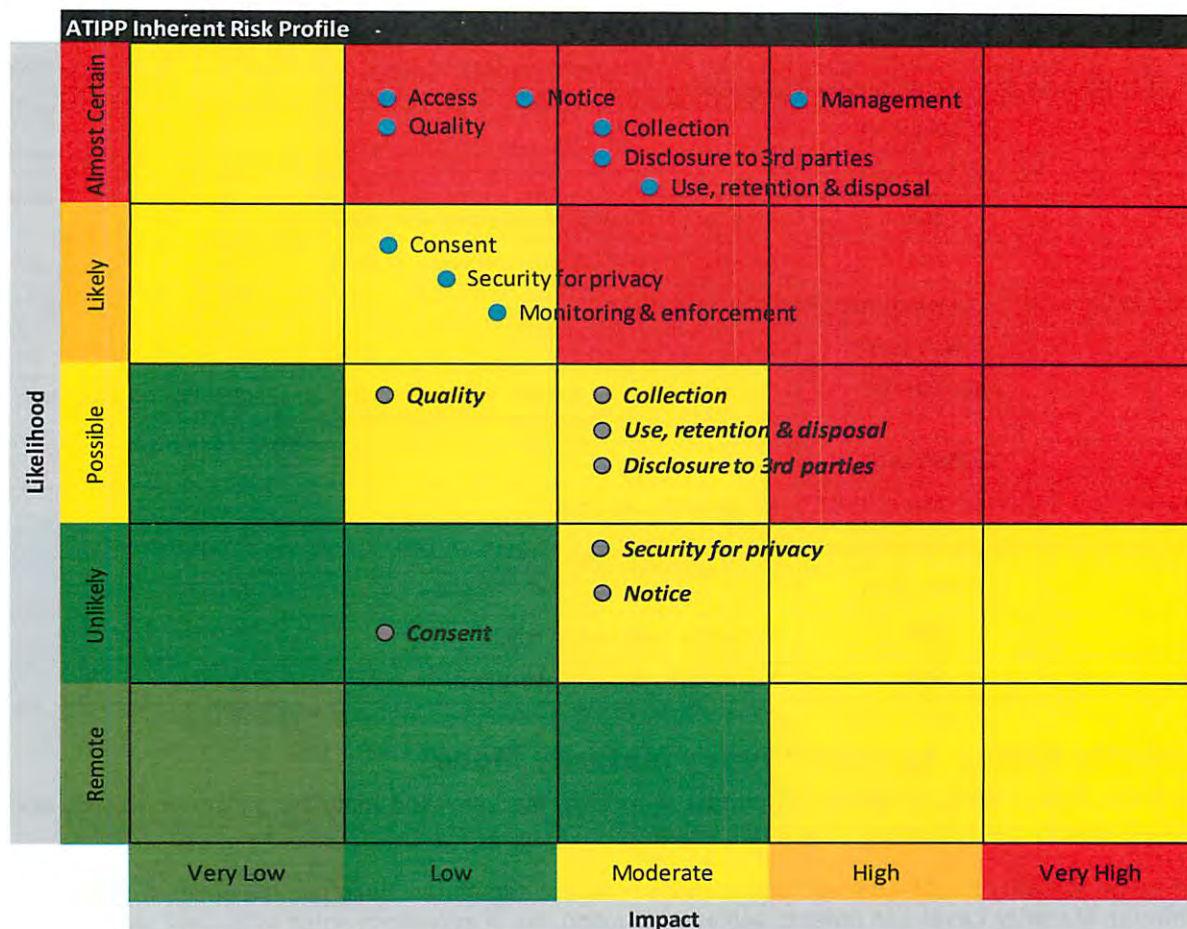
### Risk Profile

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>

## DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

#### 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
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

## DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT

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

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

#### 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	Options to strengthen ATIPP resources within ITI will be contemplated over this fiscal year and the next, subject to the GNWT fiscal planning cycle.



**DEPARTMENT OF INDUSTRY, TOURISM AND INVESTMENT**

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

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	
---	--

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

# 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 Federling

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

<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>

## **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

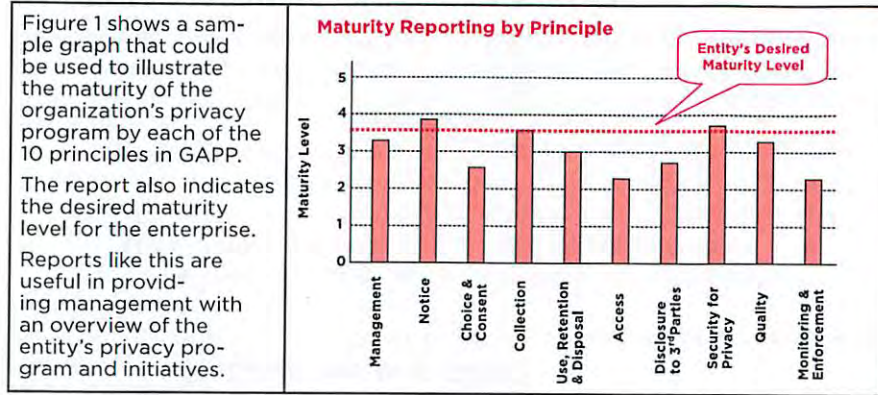


Figure 2 - Maturity Report by Criteria within a Specific GAPP Principle

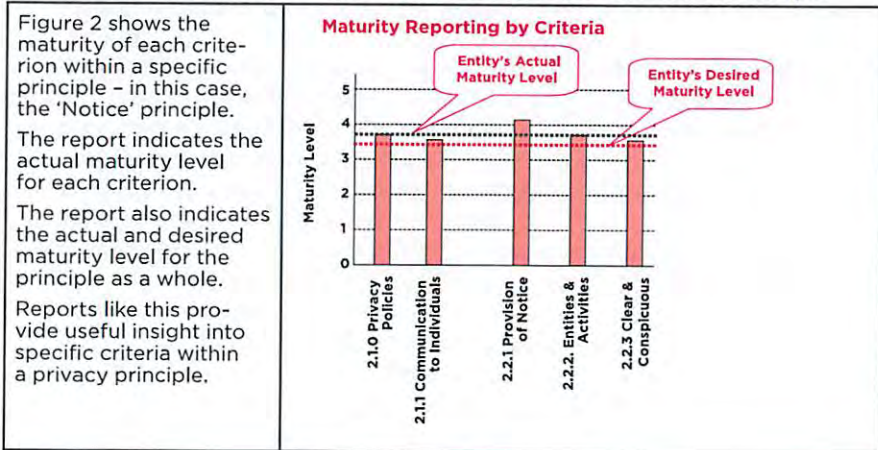
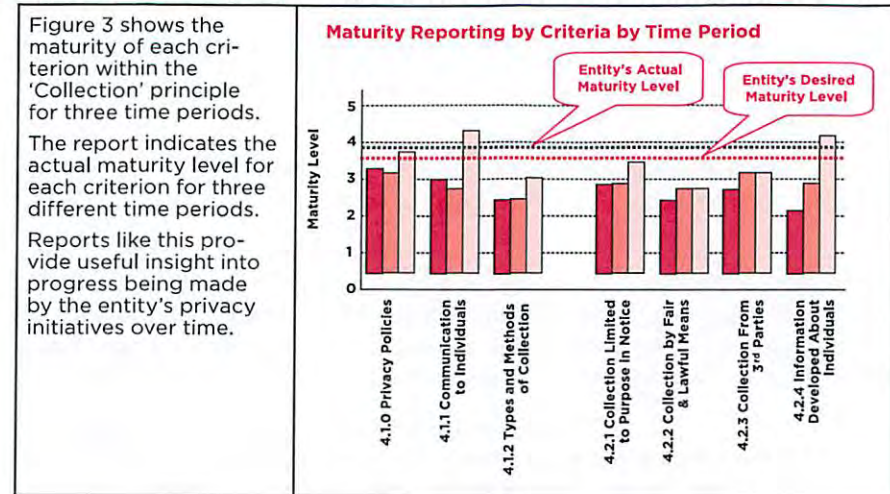


Figure 3 - Maturity Report by Criteria within a GAPP Principle Over Time



## 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.

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.

## 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>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 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>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.

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>	<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.</p>	<p>The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
<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>	<p>The entity's privacy policies address providing notice to individuals.</p>	<p>Notice policies and procedures exist informally.</p>	<p>Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented.</p>	<p>Notice provisions in privacy policies cover all relevant aspects and are fully documented.</p>	<p>Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.</p>	<p>Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance.</p>
<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>	<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.</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>	<p>Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.</p>

## Appendix A

AICPA/CICA Privacy Maturity Model

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 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>	<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 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		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.

## Appendix A

AICPA/CICA Privacy Maturity Model

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 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.

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.

## 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>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 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.

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.	The entity has developed, documented and promulgated its comprehensive enterprise-wide security program.  The entity has addressed specific privacy-focused security requirements.	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.

## 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>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>Authorizing and registering internal personnel and individuals</li> <li>Identifying and authenticating internal personnel and individuals</li> <li>Making changes and updating access profiles</li> <li>Granting privileges and permissions for access to IT infrastructure components and personal information</li> <li>Preventing individuals from accessing anything other than their own personal or sensitive information</li> <li>Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities</li> <li>Distributing output only to authorized internal personnel</li> <li>Restricting logical access to offline storage, backup data, systems and media</li> <li>Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)</li> <li>Preventing the introduction of viruses, malicious code, and unauthorized software</li> </ol>	Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete.	The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information.	<p>The entity has documented and implemented security policies and procedures that sufficiently control access to personal information.</p> <p>Access to personal information is restricted to employees with a need for such access.</p>	<p>Management monitors logical access controls, including access attempts and violation reports for files, databases and resources containing personal information to identify areas where additional security needs improvement.</p> <p>Irregular access of authorized personnel is also monitored.</p>	<p>Access and violation attempts are assessed to determine root causes and potential exposures and remedial action plans are developed and implemented to increase the level of protection of personal information. Logical access controls are continually assessed and improved.</p> <p>Irregular access of authorized personnel is monitored, assessed and investigated where necessary.</p>

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
<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 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.



## 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.







**CONFIDENTIAL**

January 16, 2019

File: 7820-20-ITI-151-131

MR. TOM JENSEN  
DEPUTY MINISTER  
DEPARTMENT OF INDUSTRY, TOURISM & INVESTMENT

**Management Letter: Royalty & Valuation of Diamonds Project**  
**Status Period: As of December 31, 2018**

---

The Audit Committee approved the management requested review of the Diamonds, Royalties and Financial Analysis Division's (Division) risk-based royalty audit process.

In May 2018, the Division engaged a consultant firm to review the Mineral Royalty Audit Manual. We recently received a copy of the consultant's final report and have no issues with this document.

The consulting project superseded the audit scope and objective approved by the Audit Committee. We provided the Division management with the planning assessment of the Mineral Royalty Audit Manual and the Canadian Audit and Accountability Foundation's, "*Practice Guide to Auditing Mining Revenues and Financial Assurances for Site Remediation*" as a reference.

We will close this file unless management requires additional information.

Sincerely,

T. Bob Shahi  
Director, Internal Audit Bureau  
Department of Finance

- c. Mr. Jamie Koe, Chair, Audit Committee  
Ms. Julie Mujcin, Director, Finance & Administration, Industry, Tourism & Investment

# Government of Northwest Territories

## Mineral Royalty Audit Manual Review

### Opportunities for Improvement

28 November 2018

# 1.0 Executive Summary

## 1.1 Objective

The objective of this project is to provide recommendations for the existing mineral royalty audit manual of DRFA (“the manual”) and develop improved processes in line with industry best practices. A clearly documented, complete and robust procedures manual is a vital governance tool. Such a document will reduce learning curves for employees, ensure continuity, promote quality assurance and efficiency, and provide our clients and stakeholders with confidence that our audit methodology is best practice.

## 1.2 Background

The Northwest Territories (NWT) is rich in mineral resources and the responsible development of these resources provides long-term economic benefits for all Northwest Territories (NWT) residents.

As of April 1, 2014, the Department of Industry, Tourism and Investment (ITI) became responsible for the administration of mineral exploration activities on public lands in the NWT.

ITI promotes economic self-sufficiency through the responsible management and development of NWT minerals to create a prosperous, diverse and sustainable economy.

ITI is responsible for:

- ▶ Policy development and planning associated with the development of the NWT’s mineral resources;
- ▶ Administration of third party rights (e.g., mineral claims); and
- ▶ Administration of royalties.

The Diamonds, Royalties and Financial Analysis (DRFA) division of the Government of the Northwest Territories (GNWT) is responsible for the collection of royalties and the audit of royalty returns submitted by mining and petroleum companies with producing facilities in the NWT. DRFA is also accountable for the administration of the royalty provisions of the Northwest Territories Mining Regulations (“the regulations”).

### 1.3 Opportunities / considerations for improvement

The opportunities / considerations for improvement within this report are broken down by the following categories of the manual:

- ▶ Introduction
- ▶ Planning
- ▶ Fieldwork

Additionally, we have included a 'General' section that speaks to broad themes that will be applicable to the entire manual.

Nine opportunities for improvement have been identified below, with guidance on suggested revision or addition. The Canadian Audit and Accountability Foundation (CAAF), Practice Guides for Auditing Mining Revenues and Financial Assurances for Site Remediation (Guide) is typically used by legislative audit organizations as a complement to their existing audit processes and procedures. These guides provide sample objectives, criteria and questions for auditing mining revenues (including royalties). This guide, along with the Institute of Internal Auditors (IIA) Standards, informed our review, and has been referenced (when applicable) and interpreted for the purpose of updating DFRA's audit manual.

### 1.4 Updated audit manual

Subsequent to providing GNWT with opportunities / considerations for improvement, we have reviewed the audit manual updates that have been drafted to address the identified opportunities listed in Section 2 below, and confirm that they do so.

## 2.0 Opportunities for improvement

### 2.1 General

Opportunity #1	The manual includes a number of templates with examples from prior audits.
Suggested revision or addition	In addition to the templates, DRFA should develop process documentation to support not only the “what” (templates), but also the “how” to guide the auditors through the process and encourage consistency.
Updated audit manual	We have reviewed several templates that have been drafted to address the opportunity above, and confirm that they do so.

Opportunity #2	The manual does not contain a quality assurance section.
Suggested revision or addition	<p>Quality assurance activities can provide additional comfort over conformance to the audit manual and other internal policies, as well as the effectiveness and efficiencies of past audits. The key considerations for having a quality assurance and improvement program includes resources availability, budget constraints, compliance requirements, etc. DRFA should document the results of their considerations on whether to include a quality assurance and improvement program in their audit regiment.</p> <p>For example:</p> <p>For each mineral royalty return audited, DRFA relies on its detailed review process (refer to the ‘Reviewing Audit Working Papers’ document in the Reporting and Review section) to ensure audit quality and conformance of audit procedures to the audit manual. Due to the small size and structure of the DRFA team responsible for auditing mineral royalty returns, DRFA has found the risk of not implementing an additional independent quality assurance and improvement program to be negligible. The formalization of lessons learned will be performed to continually improve the effectiveness and efficiencies of audits. In reviewing the manual on an annual basis to ensure continued relevance and appropriateness, DRFA will incorporate lessons learned into their applicable sections of the manual.</p>
Updated audit manual	We have reviewed the audit manual update that has been drafted to address the opportunity above, and confirm that it does so.



## 2.2 Introduction

Opportunity #3	DRFA's approach to achieving their audit objective is not defined.
Suggested revision or addition	<p>DRFA should clearly define their approach to conducting the audit/meeting the objective of the mineral royalty audits.</p> <p>As the DRFA is governed by the Northwest Territories Mining Regulations, these regulations should form the basis for:</p> <ul style="list-style-type: none"> <li>▶ Stating that DRFA audits 100% of the mineral royalty returns received from the mines producing minerals in NWT,</li> <li>▶ Describing the approach used to determine overall materiality,</li> <li>▶ Describing and justifying DRFA's higher or lower risk appetite for the different modules of the mineral royalty return,</li> <li>▶ Describing the approach used for sampling, and</li> <li>▶ Describing and justifying the extent to which reliance is placed on different types of supporting evidence (e.g., unqualified financial statements).</li> </ul>
CAAF Guidance	<p>Similar to the planning phase of an audit, the development of an overall audit approach involves acquiring knowledge of the business, assessing risk and conducting analysis. The DRFA should monitor the internal (i.e. legislation and regulations) and external (i.e. mining sector) environment for changes that may present risks for all stakeholders. These risk factors need to be assessed and responded to, as they could prevent the DRFA from effectively carrying out its responsibilities and meeting its objective.</p>
IIA Standard(s)	<p>2210 – Engagement Objectives</p> <p>Interpretation:</p> <p>Objectives must be established for each engagement.</p> <p>2210.A1 – Auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.</p> <p>2210.A2 – Auditors must consider the probability of significant errors, fraud, noncompliance and other exposures when developing the engagement objectives.</p> <p>2210.A3 – Adequate criteria are needed to evaluate governance, risk management and controls. Auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, auditors must use such criteria in their evaluation. If inadequate, auditors must identify appropriate evaluation criteria through discussion with management.</p>
Updated audit manual	<p>We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.</p>

Opportunity #4	Joint audits with INAC are included within the GNWT Royalty Audit Manual.
Suggested revision or addition	As an audit manual is a generally static document, DRFA should document the joint audits with INAC separately.
Updated audit manual	Per discussion with DRFA, the audit manual will be updated to remove the joint audit procedures as noted in the opportunity above.

Opportunity #5	The manual does not include the requirements of an audit team.
Suggested revision or addition	<p>DRFA should document the basic requirements of an audit team such as qualifications, proficiencies, independence, etc. It is important to not be overly restrictive, given the challenges of staffing in the North.</p> <p>For example:</p> <p>Dependent on the role, the audit team member should, at a minimum:</p> <ul style="list-style-type: none"> <li>➤ Have XX years of audit and/or industry experience,</li> <li>➤ Have a relevant bachelor's degree,</li> <li>➤ Have/pursuing XX certifications/designation, and</li> <li>➤ Be independent from the mine being audited.</li> </ul>
IIA Standard(s)	<p>1100 – Independence and Objectivity</p> <p>Interpretation:</p> <p>The audit activity must be independent, and auditors must be objective in performing their work. Independence is the freedom from conditions that threaten the ability of the auditor activity to carry out audit responsibilities in an unbiased manner. Objectivity is an unbiased mental attitude that allows auditors to perform engagements in such a manner that they believe in their work product, and that no quality compromises are made. Objectivity requires that auditors do not subordinate their judgment on audit matters to others. Threats to independence or objectivity must be managed at the individual auditor, engagement, functional and organizational levels.</p> <p>1200 – Proficiency and Due Professional Care</p> <p>Interpretation:</p> <p>Audits must be performed with proficiency and due professional care. Auditors must possess the knowledge, skills and other competencies needed to perform their individual responsibilities. The audit team collectively must possess or obtain the knowledge, skills and other competencies needed to perform its responsibilities. Auditors must apply</p>

	the care and skill expected of a reasonably prudent and competent auditor. Due professional care does not imply infallibility.
Updated audit manual	We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.

Opportunity #6	The manual does not define the roles and responsibilities of an audit team.
Suggested revision or addition	<p>DRFA should define the roles and responsibilities of resources at each level involved in the audit activity (i.e. outlining overall responsibilities, specific responsibilities).</p> <p>For example:</p> <p>Chief (Director) of DRFA</p> <p>The Director provides guidance and oversees all audits performed by DRFA. The Director conducts high level reviews of the audits and provides the final sign off on the Audit Report and Letters.</p> <p>Manager</p> <p>The Manager reports to the Director of DRFA and takes the lead in planning and overseeing all phases (i.e. planning, fieldwork and reporting) of the audit. The Manager works closely with the client and is responsible for supervising the audit team.</p> <p>Auditor</p> <p>The Auditor reports to the Manager and is involved in all phases of audit activity (i.e. planning, fieldwork and reporting) under their supervision. The auditor will perform detailed testing and documentation review and will support the audit team by taking notes in interviews and meetings.</p>
IIA Standard(s)	<p>2230 – Engagement Resource Allocation</p> <p>Interpretation:</p> <p>Auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints and available resources. Appropriate refers to the mix of knowledge, skills and other competencies needed to perform the engagement. Sufficient refers to the quantity of resources needed to accomplish the engagement with due professional care.</p>

	<p>2340 – Engagement Supervision</p> <p>Interpretation:</p> <p>Engagements must be properly supervised to ensure objectives are achieved, quality is assured and staff is developed.</p>
Updated audit manual	We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.

### 2.3 Planning

Opportunity #7	Formalization of guidance on performing risk assessments.
Suggested revision or addition	<p>The Preliminary Survey Template document in the planning section of the manual consists of the results of a risk assessment, but does not include guidance on how the risk assessment was performed. DRFA should formalize guidance on how to perform risk assessments that will enable an auditor to gain insight, perspective and other pertinent information that will lead to establishing audit priorities. For example, the guidance may include how the following activities will be performed as part of the risk assessment:</p> <ul style="list-style-type: none"> <li>▶ Interview key stakeholders,</li> <li>▶ Gather relevant historical and current financial information,</li> <li>▶ Identify where there is a lack of information available to the auditor,</li> <li>▶ Identify areas which may warrant further investigation,</li> <li>▶ Perform quantitative and qualitative analysis, and</li> <li>▶ Validation, synthesis and analysis of findings.</li> </ul>
CAAF Guidance	<p>The practice guide states that, in order to establish the audit focus, the auditor must conduct further research in areas identified as relevant and important (i.e. perform a risk assessment). The guide provides a sample of high-level questions that the DRFA can research to determine the extent to which the audit will focus on revenues from the extraction of minerals. These include:</p> <ul style="list-style-type: none"> <li>▶ What is the variance between forecasted and actual revenues? Is there an explanation? Is it in line with current market conditions and production levels?</li> <li>▶ Is there new legislation or regulation? Have there been recent significant changes made to existing legislation or regulation?</li> <li>▶ Do the financial statements identify any issues related to the collection of revenues?</li> </ul>

	While the list of questions are not exhaustive, lines of inquiry at this level can direct an auditor's focus to higher risk sections of a mining royalty return.
IIA Standard(s)	2201 – Planning Considerations  Interpretation:  In planning the engagement, auditors must consider <ul style="list-style-type: none"> <li>- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.</li> <li>- The significant risks to the activity's objectives, resources and operations, and the means by which the potential impact of risk is kept to an acceptable level.</li> <li>- The adequacy and effectiveness of the activity's governance, risk management and control processes compared to a relevant framework or model.</li> </ul>
Updated audit manual	We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.

## 2.4 Fieldwork

Opportunity #8	Formalization of risk-based sampling methodology and procedures.
Suggested revision or addition	DRFA should document the sampling approach, why it is performed, the methodology being undertaken and how it is to be applied across the different categories of transactions. Document in detail DRFA's step by step process of risk-based sampling. Where applicable, detail the NWT mining regulations section(s) that support the sampling rationale.  Documenting the rationale and approach behind the sampling methodology will not only guide a reader on how to perform risk-based sampling, but enable consistency across audits.  Refer to Appendix 3.1 for an example of a sampling memo.
Updated audit manual	We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.

Opportunity #9	Additional working paper details.
Suggested revision or addition	DRFA can include additional details such as population and sample size rationale, test procedures, risks, conclusions, notes/comments, etc., to provide clarity and insight that could help facilitate completeness of work, more easily align procedures and risks, and support the review process of the audit file.

	Refer to Appendix 3.2 for an example of a working paper.
IIA Standard(s)	<p>2330 – Documenting Information</p> <p>Interpretation:</p> <p>Auditors must document sufficient, reliable, relevant and useful information to support the engagement results and conclusions.</p>
Updated audit manual	We have reviewed the audit manual updates that have been drafted to address the opportunity above, and confirm that they do so.

## 3.0 Appendices

### 3.1 Example sampling memo

#### Sampling Methodology and Selection

**Audit Criterion 2.2:** Key controls, within the travel processes, are operating effectively to support accuracy and appropriateness of transactions, including external reporting.

**Audit Procedure 2.2.1:** Perform detailed testing of key controls within the travel expenditure process to determine if controls are operating effectively and in compliance with policies.

Criterion 2.2 requires sampling to complete the planned audit steps. The general methodology that will be applied to all samples is based on the following:

- Internal audit has conducted a risk assessment for the processes that encompass travel management, through walkthroughs with key personnel and documentation review. Using professional judgement, the audit team has assessed the travel management controls as having limited inherent risk of material non-compliance due to the following factors:
  - Policies and procedures exist for different types of travel management activities; and, in general, travel management activities are routine.
  - Travel management was previously audited in 2016 and there were no high priority findings. In addition, the process has not changed substantially since the 2016 audit. However, in the 2016 audit, there were several instances of non-compliance with policy found during testing, especially with respect to non-staff travel. Management conducted training, developed tools and implemented periodic monitoring procedures to reduce the likelihood of errors occurring in the future.
  - No significant concerns or risks were identified during the planning phase.
  - The external auditor included executive and board travel and hospitality expenses in their 2017-2018 annual financial audit and found no significant concerns.
- **Sampling Approach:** Based on Internal Audits sampling methodology, a judgemental sample (non-statistical) will be used. The audit will not extrapolate the results throughout the entire population. The data will be reviewed and judgement will be exercised in an attempt to select a representative sample that includes expenses from both Location1 and the regional offices to ensure different interpretations of the policies and procedures are tested. Priority will be given to high dollar value expenses, when selecting samples. Testing will identify common risk themes and, if a theme or commonality is identified that poses a risk, additional testing may be conducted.
- **Type of Sampling Plan:** Control (attribute) testing given that the population is nonmonetary. In this type of sampling, the audit will be examining documentation and information (called an attribute) that supports the assertion that the control is effective (functioning as intended).
- This audit will focus on the controls within the travel management part of the process and will not test controls within the payment process of travel expense claims. The process to pay a travel expense claim is part of the standard corporate accounting payment process, which was tested in another Audit.

Specific information for determining populations and samples is detailed below.

#### Sample Selection – Staff, Non-staff, and other

18(a)

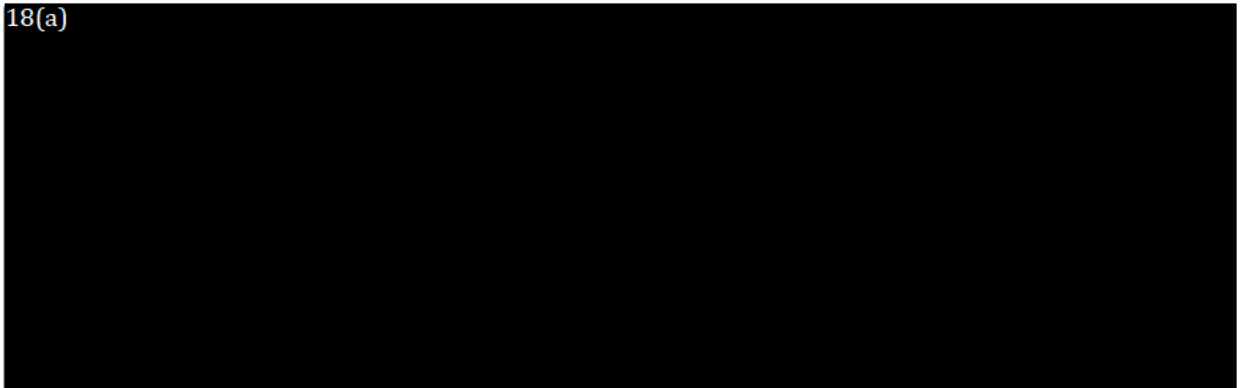


18(a)

A large black rectangular redaction box covering the majority of the page content.

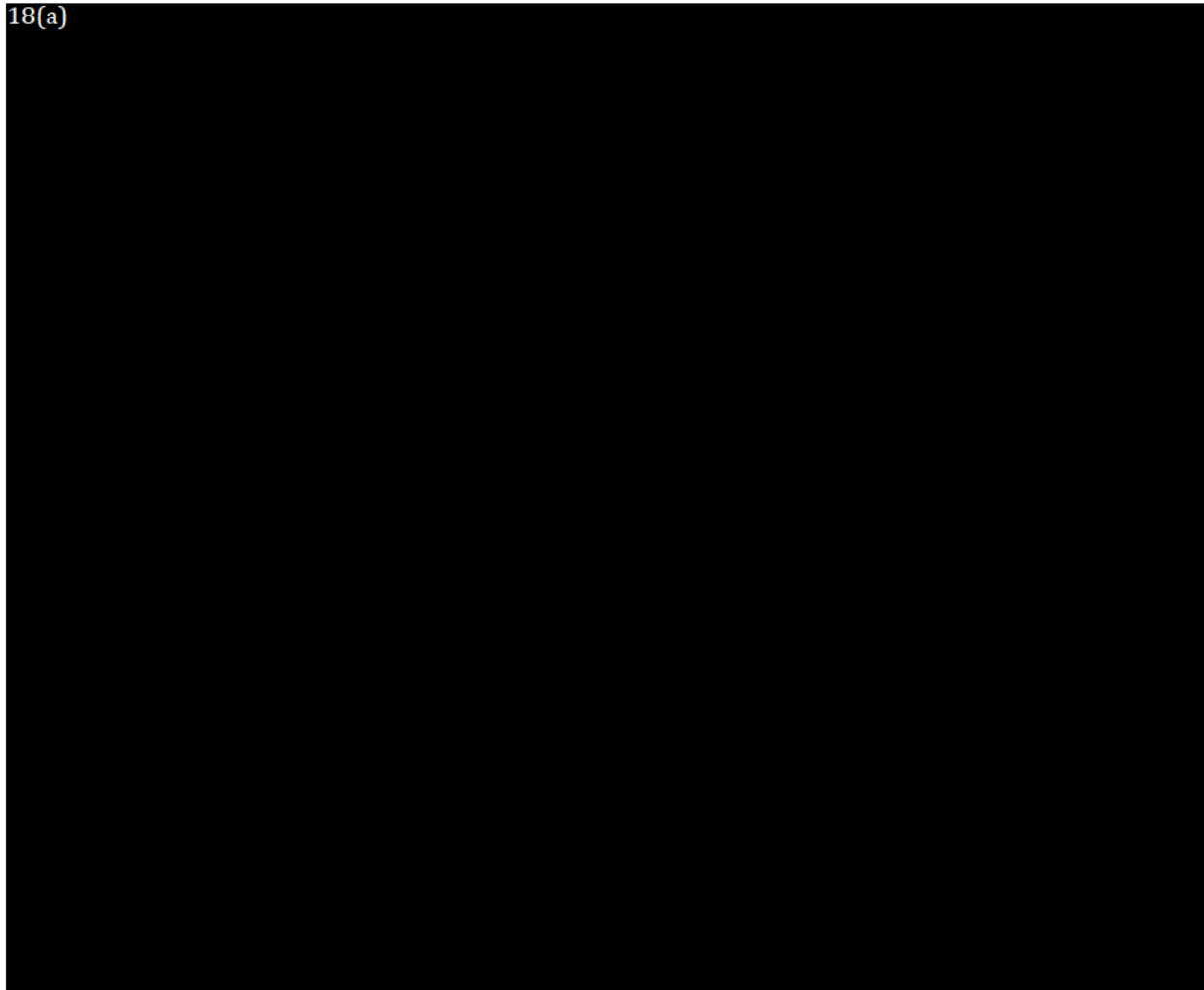
**Completeness of population**

18(a)

A large black rectangular redaction box covering the majority of the page content.

**Population determination**

18(a)

A large black rectangular redaction box covering the majority of the page content.

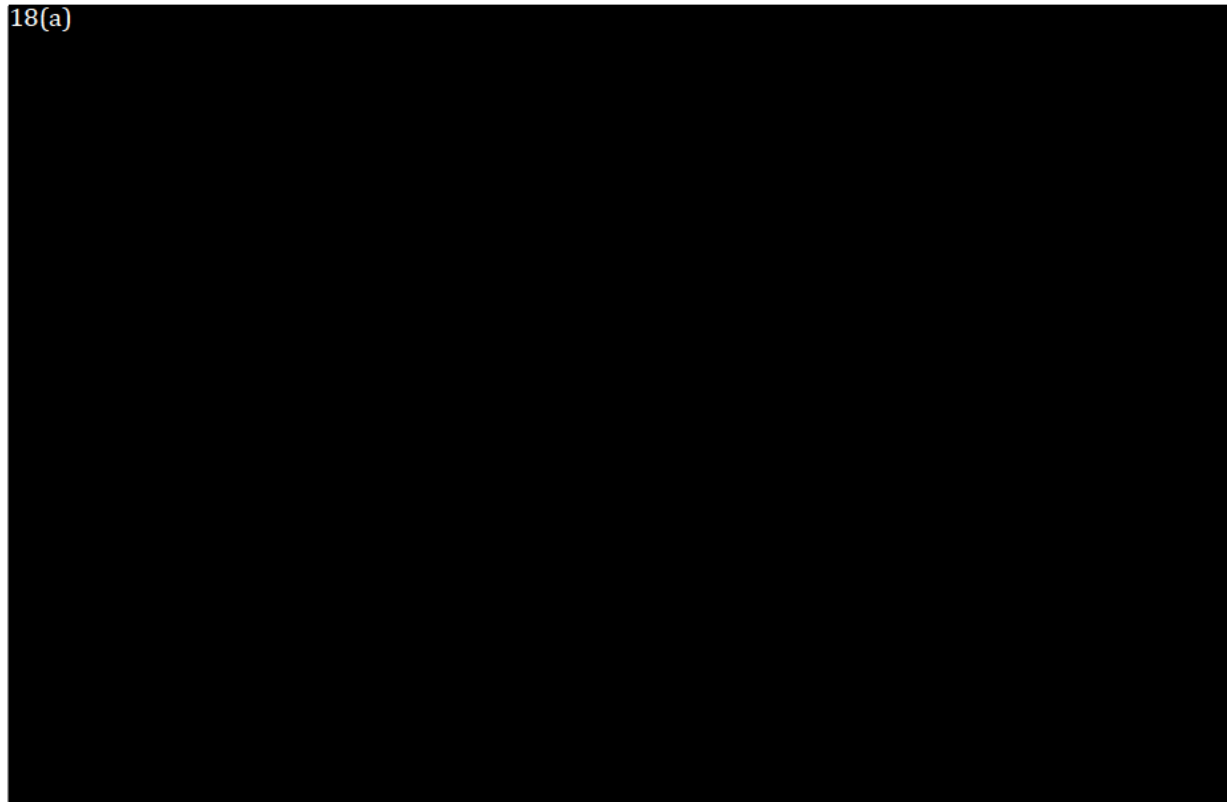




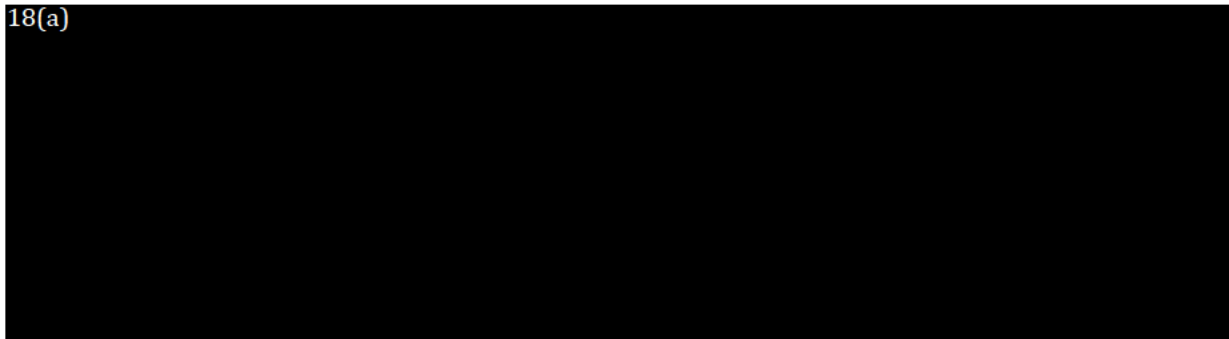
**Sampling methodology**

Staff and Non-staff travel expenses

As per Internal Audit's internal audit sampling methodology, when controls are moderately significant and there is a limited inherent risk of material noncompliance for populations of 250 items or greater, 25 is the appropriate sample size.




18(a)

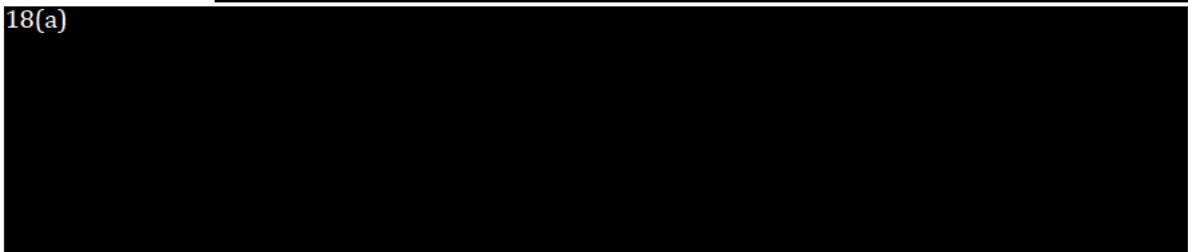


Other travel expenses

In accordance with Internal Audit sampling methodology, for small populations between 24 and 52, a sample size of 5-9 should be tested. This is also subject to professional judgment, which considers the risk assessment. 18(a)

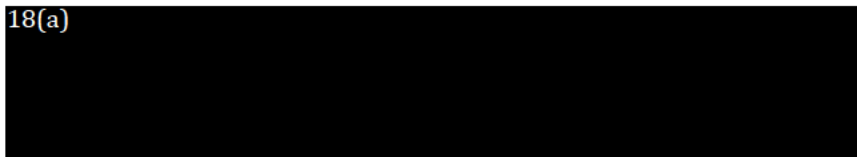


18(a)



**Sampling Unit:**

18(a)



**Sample Selection – Corporate Accounting Reconciliations**

18(a)



**Completeness of population**

18(a)



**Population determination**

18(a)



**Sampling methodology**

Per Internal Audit sampling methodology, controls that do not occur frequently (i.e. quarterly) have a sample size of 2.

**Sampling unit**

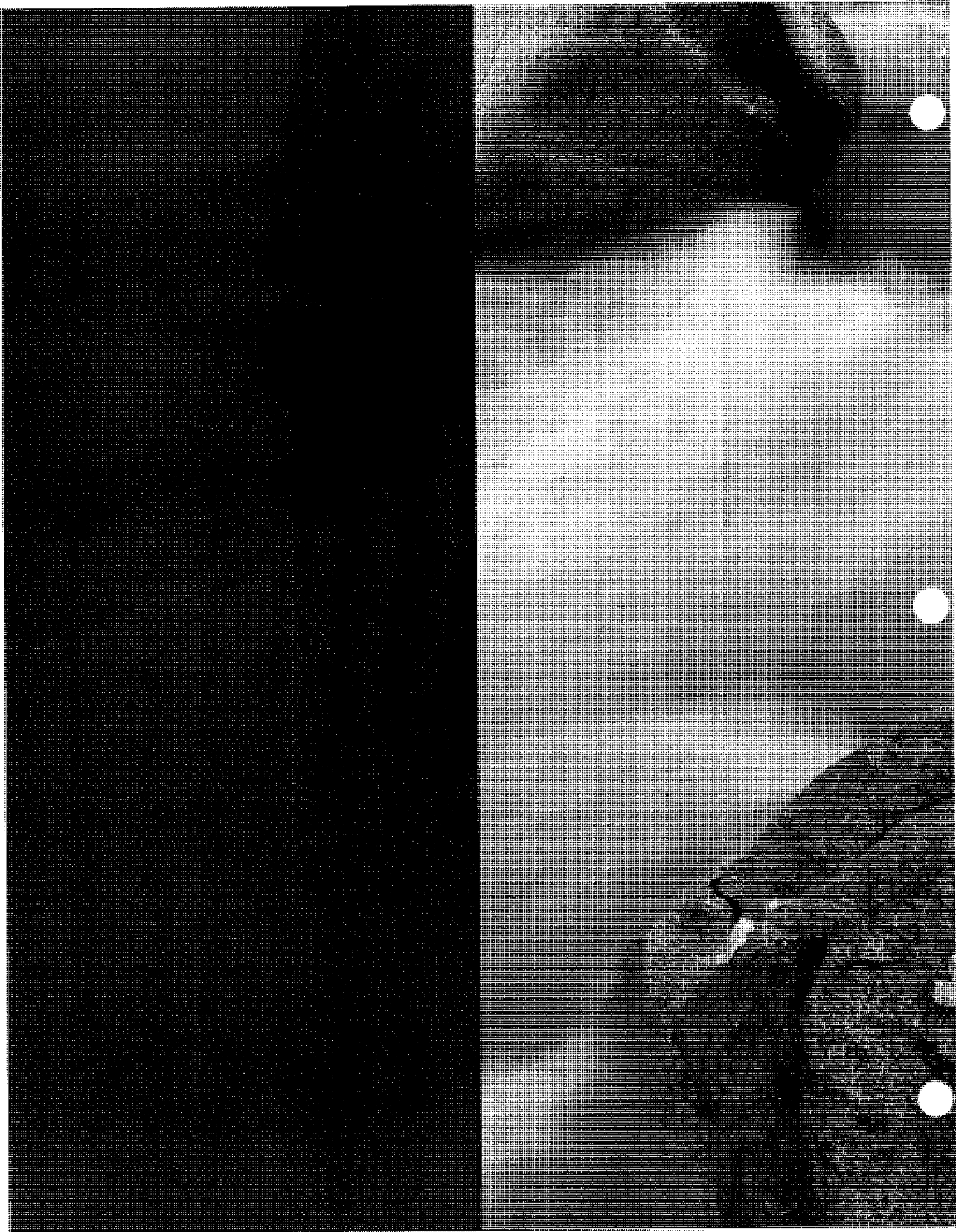
18(a)



### 3.2 Example working paper

**Diamonds, Royalties and Financial Analysis (DFRA)**  
**Mineral Royalty Return Audit (Organization, Date)**  
 WP reference: <Insert file reference>  
 Prepared by: <Auditor, DFRA, date>  
 Reviewed by: <Manager, DFRA, date>

General							
Purpose		<Define the purpose of this working paper; reference regulation section if applicable >					
Audit Criteria		<Define the audit criteria>					
<b>Testing strategy</b>							
Population source and details		<Provide details on the nature of the population (i.e. GL expense listing) and its source (i.e. client ERP system, manual listings, etc.), refer to additional working papers/tabs for full population listing>					
Scope period		<Detail the testing period>					
Population size		<Detail the population size>					
Sample size		<Detail the sample size>					
Sample selection methodology		<Detail the sampling approach, refer to additional working papers/tabs for procedures performed on the population(s) for sampling, reference DFRA's sampling methodology document or audit manual>					
<b>Testing procedure</b>							
					Substantive test - refer to next section for description		
Testing #	Sample #	Royalty Return Section or Category	Reference #	Other sample identifiers	A	B (if required)	Ref
1	<#>	<i.e. processed minerals, general administration expenses>	<#>	<identify>	<Detail the results of sample testing using procedure A>	<Detail the results of sample testing using procedure B>	<evidence reference, if applicable>
<b>Procedure(s)</b>							
A		<Develop testing procedure to satisfy audit criteria>					
B		<Develop additional testing procedure to satisfy audit criteria, if required>					
<b>Conclusion</b>							
Overall conclusion		<Detail the audit criteria and results of testing against these criteria>					
Exceptions noted during testing		<If applicable, provide detail around exceptions to test procedures>					





**CONFIDENTIAL**

File: 7820-20-ITI-151-130

MR. TOM JENSEN  
DEPUTY MINISTER  
INDUSTRY, TOURISM & INVESTMENT

**ITI Territorial Parks Contracts Management**

Enclosed is the above referenced Audit Report.

Management's response, proposed action plan and target completion dates have been included in this report. We will schedule a follow-up in the future to assess the progress on the Management Action Plan. However, we would appreciate an update by December 2016 on the status of the action plan.

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

T. Bob Shahi  
Director

Enclosure

- c. Mr. Jamie Koe, Chair, Audit Committee
- Mr. Jamie Koe, Comptroller General, Finance
- Ms. Julia Mujcin, Director, Finance & Administration, ITI



## ITI, Territorial Parks Contract Management

Internal Audit Bureau – Audit Report



## **Audit Report Operational Audit**

### **Industry, Tourism & Investment Territorial Parks Contracts Management**

**October 2016**

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



**CONFIDENTIAL**

October 5, 2016

File: 7820-20-ITI-151-130

MR. TOM JENSEN  
DEPUTY MINISTER  
INDUSTRY, TOURISM & INVESTMENT

**Audit Report: ITI Territorial Parks Contracts Management**  
**Audit Period: April 1, 2015 – November 30, 2015**

---

**A. SCOPE AND OBJECTIVES**

The Audit Committee approved the Department of Industry, Tourism and Investment (ITI) management request for an audit of the territorial parks management contracts as part of the 2015-2016 audit work plan.

The audit objectives were to assess the GNWT Territorial Parks operational contracts, in terms of the Governance Framework, Reliability and Integrity of Information, Compliance, Asset Safety and Efficiency and Effectiveness.

The audit scope covered the period from April 1, 2015 to November 30, 2015. All transactions and operations related to the Territorial Parks' contracts during this time period were considered within the audit scope.

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



## **B. BACKGROUND**

Section 6 of the Territorial Parks Act empowers the Minister to enter into agreements with persons, sole proprietorships, societies, associations, partnerships, municipalities or other bodies to operate and maintain the territorial parks. At the time of the audit, ITI was directly responsible for the management of 15 parks, while 19 parks were managed by independent contractors. The audit focused on the management contracts established with the 19 independent contractors.

The audit contract was awarded to Grant Thornton by a Request of Proposal evaluation team composed of ITI and Internal Audit Bureau (IAB) staff. An IAB auditor was assigned to support the work of the contractor.

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

The attached report by Grant Thornton *Audit of Territorial Parks* made a number of observations and 17 recommendations.

Four recommendations did not require any additional action as internal controls were already implemented to mitigate the identified risk or management has accepted the risk:

- 1) Reporting and reconciling of revenue
- 2) Data integrity of historical financial transactions
- 3) WSCC requirements relevant to park operations
- 4) Payments to contractors are in accordance with contract.

Management developed action plans to address the risk identified in 9 areas covering 13 recommendations:

- 1) Invoicing requirements for contractors
- 2) Revenue recognition and forecasting
- 3) ORS user access manual and prescribed role functionality
- 4) Conducting and documenting park inspections
- 5) Park signage updating
- 6) Emergency procedure updating.

The IAB will follow-up on the status of the management action plan for the 13 recommendations during our scheduled follow-up audits.

#### **D. ACKNOWLEDGEMENT**

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

Sincerely,

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

T. Bob Shahi  
Director

# Government of the Northwest Territories

Department of Finance



Final Report

## Audit of Territorial Parks

---

March 31, 2016

## TABLE OF CONTENTS

1.	<b>EXECUTIVE SUMMARY</b> .....	3
1.1	<b>Background / Context</b> .....	3
1.2	<b>Audit Objectives and Scope</b> .....	3
1.3	<b>Summary of Observations and Recommendations</b> .....	4
2.	<b>DETAILED AUDIT REPORT</b> .....	9
2.1	<b>Introduction and Background:</b> .....	9
2.2	<b>Focus of the Internal Audit:</b> .....	9
2.3	<b>Observations:</b> .....	10
	<b>APPENDIX A – AUDIT CRITERIA</b> .....	21
	<b>APPENDIX B –FAM REQUIREMENTS</b> .....	22
	<b>APPENDIX C – FINDINGS RATING SCALE</b> .....	25

## 1. EXECUTIVE SUMMARY

### 1.1 Background / Context

In December 2015, the Government of Northwest Territories (GNWT) engaged Grant Thornton LLP (GT) to conduct an operational audit of the GNWT Territorial Parks. Under the responsibility of the Department of Industry, Tourism and Investment (ITI), there are a total of 41 territorial parks located across five (5) different regions. Of those 41 parks, 19 are managed by independent contractors. The value of the 19 Park Operation Contracts issued to 17 contractors totaled \$1,095,309 for the 2015 park season as summarized in the table below (information in the table was provided by ITI).

Region	# Parks Managed by Contractors	Contractors	Total Paid to Contractors (2015)	% of Total Paid to Contractors (2015)
Beaufort Delta	5	Midnight Sun Contracting, MGM Bus Service, Alexie Enterprises	\$179,381	16.38%
Sahtu	0	NA	\$0	0%
North Slave	4	Bottom Line PR, Gilbert Tatzia, Endeavoursome 2000 Ltd., Al and Mary Morton Ltd.	\$449,660	41.05%
Dehcho	3	B.J. Contracting, R.W. Contracting, Cli-Michaud Contracting	\$160,444	14.65%
South Slave	7	Ev's Enterprises, Undah Gogah Corporation, Eagle 88 Ltd., Noda Enterprises, Det'an Cho Tourist Camp, P&T Contracting, RC Renovations	\$305,824	27.92%
<b>Total</b>	<b>19</b>	<b>17</b>	<b>\$1,095,309</b>	<b>100%</b>

Park Operation Contracts are procured annually and many contracts include the option to renew for two seasons, making the total contract period up to three (3) years. The park contractors are responsible for the activities related to operating the Territorial parks, including but not limited to, managing and issuing park permits, collecting and reconciling cash, reporting on cash collected, sanitary maintenance of the park and its facilities, dealing with the public, and hosting activities at the park.

### 1.2 Audit Objectives and Scope

The objective of this audit was to assess the GNWT Territorial Parks operational contracts, in terms of the Governance Framework, Reliability and Integrity of Information, Compliance, Asset Safety and Efficiency and Effectiveness.

Our audit scope covered the period from April 1, 2015 to November 30, 2015. All transactions and operations related to the Territorial Park contracts during this time period were considered within the audit scope.

### 1.3 Summary of Observations and Recommendations

We identified a number of positive observations as well as opportunities for improvement. Detailed findings can be found in section 2.0 of the report.

The following positive observations were identified through the audit:

- Park contractors have appropriate, segregated access to the On-line Reservation System (ORS).
- Territorial park assets are regularly inspected and reported on.
- There is formality and segregation of duties around the processes for accounting and reporting on assets.
- Emergency protocols and procedures are in place in Deh Cho and North Slave.

In addition to the positive observations above, four (4) key observations, including opportunities for improvement, were identified during the audit. The table below classifies and prioritizes the findings according to the impact on the organization (extreme, high, medium, minor or insignificant as defined in Appendix C – Findings Rating Scale).

Audit Area	Key Observations	Impact Assessment	Report Section
1. Governance	■ Revenue Reporting and Invoicing	High	2.3.1
2. Reliability and Integrity of Information	■ Online Reservation System – access and reliability	High	2.3.2
3. Compliance	■ FAM sections 4.2.2, 4.2.4, and 4.2.6	Extreme	2.3.3
	■ WSCC – new regulations (June 2015)	Medium	
	■ Territorial Parks Act	Medium	
	■ Emergency Protocol	Medium	
4. Assets and Visitor Safety	No key observations	NA	2.3.4
5. Efficiency and Effectiveness	■ Contracting Practices	Minor	2.3.5

Our findings and recommendations are summarized below and further described in section 2.3 – Observations.

#### Key Observation 1: Revenue Reporting / Invoicing

Park contractors collect revenue from park operations, including but not limited to the issuance of permits, kitchen and shower rentals, and firewood sales. The cash collected through park operations is retained by the contractor as payment for services and then netted against the contract amount. Contractors are required to submit regular invoices to report revenue collected against the contract amount. Any net differences between cash collected via park operations and contracted amounts are paid to the contractors, or conversely from contractors to the GNWT.

The park managers are responsible to review the invoices, perform reconciliations and approve any payments made to contractors. This function was in place and there was evidence of review and approval from the park managers. However, between regions there were inconsistencies in the frequency of invoices submitted by contractors:

- For two (2) of the four (4) regions tested, the contractor submitted invoices monthly.
- For the other two (2) regions tested, the contractor submitted one (1) final invoice for the contract, at the end of the park season.

Furthermore, there was no formal, macro-level analysis of the park revenues, particularly the “other” revenues generated by the parks, such as kitchen rentals, showers, and vehicle permits, to help ensure completeness of revenue reported.

**Recommendation 1:**

We recommend that:

- A. All contracts require that park operators submit monthly invoices, reporting on revenues collected with complete back-up support for all revenues reported. At a minimum invoices should include the following:
  - Invoice number
  - Invoice date
  - Invoice period (what dates are covered by the invoice)
  - Detail on revenue collected, separated by revenue stream and supported by back up that reconciles to the revenue reported in the invoice
  - Invoice total
  - Payment terms
- B. Industry, Tourism and Investment (ITI) Park Management reconciles the invoices on a monthly basis to validate that documentation is maintained to support the revenues reported.
- C. Additional controls are developed and implemented to help ensure completeness of revenue. For example, establish revenue forecasts by park and including forecasts for “other” revenues activities. To further illustrate the example, if a kitchen shelter is available for rental for the park season management could estimate that it would be rented “X”% of the time, which would represent “X” in revenues. Compare these forecasts against actual revenues reported and follow-up on major discrepancies.

**Key Observation 2 – Online Reservation System (ORS)**

The public can purchase park passes via the On-line Reservation System (ORS). A third-party company, Outcrop, manages and maintains the ORS.

During the audit, a walkthrough was performed with Outcrop staff. The walkthrough validated that the Park operator’s access to the ORS system is reasonable and appropriately segregated. However, it was noted that a formal document prescribing user access by role is not in place.

Additionally, the audit included a walkthrough of the ORS to review the accuracy and reliability of the data. The walkthrough found an error related to the refund function:

- After the refund was performed, a report was run to review the revenue and the refunded amounts. Instead of netting the amounts (e.g. \$100 Park Pass less refund of \$90 = \$10) the amounts were added together (e.g. \$100 Park Pass + Refund of \$90 = \$190), totaling an incorrect number. This demonstrated a system error impacting system reliability and data accuracy.

**Recommendation 2:**

We recommend that:

- A. ITI leverage the internal informatics shared services department to liaise with Outcrop and ITI Management to provide some IT oversight and expertise regarding the ORS.

- B. Management develop a user access listing prescribing the functionality and access required by role. Access levels should be periodically reviewed.
- C. Management conduct a review of historical data to ensure that that the system “glitch” found has not impacted payments made to contractors. Additionally, management should confirm with Outcrop that the system “glitch” has been addressed.

### **Key Observation 3: Compliance**

The audit reviewed GNWT’s compliance with a number of legislative and regulatory requirements related to the operation of Territorial Parks. Specifically this included the Financial Administration Manual (FAM), the Territorial Parks Act, the Workers Safety and Compensation Commission (WSCC) and Emergency Protocols. The following observations were made regarding compliance to the above-noted regulations:

**FAM:** It was found that the FAM requirements related to revenue collected at the Parks, specifically sections 4.2.2, 4.2.4, and 4.2.6, were not being adhered to due to the fact that contractors collect all revenues generated through park operations and then net the revenues from the total contract value. As such, the revenues collected by the contractors have been classified by ITI as the contractor’s revenue. The audit did not identify any evidence of approval or authority for the system of netting revenues and FAM exemption.

**Territorial Parks Act (Regulations):** Park Officers conduct park inspections and complete park inspection forms detailing the results of the inspections. A sample of park inspection forms was requested for all 19 parks that have Park Operation Contracts to validate that the Park Officers assess and report on compliance with the Act. Of the 19 parks from which we requested samples, 16 provided the requested park inspection forms. However, none of the 16 inspection forms tested included evidence that the key requirements of the Territorial Park Act Regulations (i.e. sections 16.1 required quiet time, 8(2) vehicles/trailers parked in designated areas, 5.1, 6, 6.1 adherence to fire requirements, 5 garbage and waste and 17 review of permits issued) were assessed during the inspections.

Finally, a walk-through was performed at three (3) territorial parks (Prelude Lake, Fred Henne and Fort Simpson) to validate that signage was displayed in both official languages. Of those three (3) parks, only one (1) (Fred Henne) displayed some signage in both English and French, all other signs displayed English only.

**WSCC:** Interviews conducted stated that the new WSCC requirements (June 2015) have not yet been implemented, and as such, the processes surrounding the requirements for contractors to track safety, training, and inspections of parks, related to health and safety of employees, have not been set-up, formalized or communicated to the contractors.

**Emergency Protocols:** Three (3) of the four (4) regions were found to have emergency protocols in place, with protocols that are formalized and communicated. However one (1) region had no real protocols in place, aside from a listing of emergency contact phone numbers.

Additionally, the audit performed testing to review the quality of the invoices submitted by the contracted park operators with respect to accuracy, completeness and timelines. A sample of eight (8) contractor invoices representing all four (4) regions where there are contractors, were selected for testing. Testing results found that:

- For six (6) of the invoices, there was insufficient information provided by the contractor to support the revenue amounts reported on the contractor invoices, including;
  - Back up support provided did not reconcile to the revenue amounts reported on the invoices, and
  - Insufficient and/or no back-up support provided to validate the revenue amounts on the invoices.





- For two (2) invoices tested, contractors were paid for an amount that exceeded the parameters of the original contract (excess amount represented \$26,372). Park management had a rationale for these additional amounts but no formal documentation or contract amendments were provided.

**Recommendation 3:**

We recommend that:

- A. The “revenue netting” process is reviewed and a formal decision to continue or discontinue this process is confirmed. Additionally, we recommend that the FAM requirements relevant to the operations of the territorial parks (including sections 4.2.2, 4.2.4, and 4.2.6) are identified, and processes compliant with the FAM requirements are set up, clearly communicated to park contractors, and are included in the contracts, where applicable.
- B. The WSCC requirements relevant to the park operations are identified and that processes are communicated to and implemented by the park contractors in compliance with the regulations.
- C. Park inspections be completed and documented at regular intervals.
- D. Park inspection forms be updated to include evidence of review of the key Territorial Park Act requirements.
- E. The park signage be updated and include the use of graphic and symbolic signage, similar to some of the signage currently used in Fort Simpson.
- F. Payments made to park operators are in-line with the contract amounts. If additional payments are required, a formal contract amendment is procured and approved. (See recommendation 1 for additional recommendations related to the invoicing process)
- G. Emergency protocol procedures are updated to be consistent in all four (4) regions.

**Key Observation 4: Contracting**

The audit assessed 19 Territorial Park contracts, representing all parks operated by independent contractors, to determine if the contracting terms and conditions and general contracting practices were in-line with public sector practices.

Key findings included:

**Invoicing:** The contracts did not consistently specify the invoicing requirements, including the frequency of invoicing, the templates, format to be used, and back-up support that should be provided to support the invoice.

**Online Reservation System (ORS):** The ORS is meant to capture all revenues collected by the contractors; including online payments made directly through the ORS, and revenues collected at the gate for permits, kitchen rentals, among others. The contracts do not state that all revenues must be input into the ORS, along with required timelines and regular reporting requirements.

**Regulatory Compliance:** The contracts did not include requirements or procedures to ensure that the contractors are in compliance with the new occupational health and safety (OHS) regulations established in June 1st, 2015 by the Workers Safety and Compensation Committee (WSCC). Additionally, FAM requirements and procedures have not been documented or included in the park contracts, with respect to the requirements related to sections 4.2.2, 4.2.4, and 4.2.6.

**Plain Language:** During the audit, Park Management indicated that some of the contractors have difficulty with the legal nature of the contract language. The contract could be written in plain language to improve comprehension of the terms.



**Recommendation 4:**

We recommend that management update their standard terms and conditions within their contracts to include:

- A. Clear invoicing requirements that include billing procedures, frequency of reporting, templates to be used, back-up support to be provided.
- B. Requirements to update the ORS on a regular, timely basis.
- C. See recommendation #3 for regulatory requirement updates.
- D. We recommend that Park Contracts be written in plain language to improve comprehension of the contract terms.

## 2. DETAILED AUDIT REPORT

This section presents the detailed findings from the Territorial Parks audit. Findings are based on the evidence and analysis from our initial risk analysis and execution of the detailed audit work program.

### 2.1 Introduction and Background:

In December 2015, the Government of Northwest Territories (GNWT) engaged Grant Thornton LLP (GT) to conduct an operational audit of the GNWT Territorial Parks. Under the responsibility of the Department of Industry, Tourism and Investment (ITI), there are a total of 41 territorial parks located across five (5) different regions. Of those 41 parks, 19 are managed by independent contractors. Contracts are procured annually and many contracts include the option to renew for two seasons, making the total contract period up to three (3) years.

The value of the 19 contracts totaled \$1,095,309 for the 2015 park season. As outlined in the chart below, the North Slave region represents 41.05% contracted amounts paid to contractors, followed by South Slave, representing 27.92% of the contracted amounts paid. The table below depicts a summary of the contracts, by region, including number of parks and amounts paid out to contractors (information in the table was provided by ITI).

Region	# Parks Managed by Contractors	Total Paid to Contractors (2015)	% Total Paid to Contractors (2015)
Beaufort Delta	5	\$179,381	16.38%
Sahtu	0	\$0	0%
North Slave	4	\$449,660	41.05%
Dehcho	3	\$160,444	14.65%
South Slave	7	\$305,824	27.92%
<b>TOTAL</b>	<b>19</b>	<b>\$1,095,309</b>	<b>100%</b>

The park contractors are responsible for the activities related to operating the Territorial parks, including but not limited to, managing and issuing park permits, collecting and reconciling cash, reporting on cash collected, sanitary maintenance of the park and its facilities, dealing with the public, and hosting activities at the park.

The park season varies slightly from region to region based on park accessibility, but the season typically runs from May through September.

### 2.2 Focus of the Internal Audit:

The objective of this audit was to assess the GNWT Territorial Parks operational contracts, in terms of the Governance Framework, Reliability and Integrity of Information, Compliance, Asset Safety and Efficiency and Effectiveness.

Our audit scope covered the period from April 1, 2015 to November 30, 2015. All transactions and operations related to the Territorial Park contracts during this time period were considered to be within the audit scope.

Site visits were conducted in two (2) regions – North Slave (Yellowknife) and Deh Cho (Fort Simpson), representing three (3) parks, Fred Henne, Prelude and Fort Simpson, where process walkthroughs, audit testing and interviews were completed. Additionally, our testing methodology selected samples from the other regions/ parks to provide an overall representative sample for key controls and procedures, to the extent possible.

### **2.3 Observations:**

Findings are based on the evidence and analysis from both our initial risk analysis and the execution of the audit work program. Observations are presented below by line of inquiry. Please refer to Appendix A for audit criteria and sub-criteria.

#### **2.3.1 Governance**

The audit reviewed and tested if reconciliations were performed at regular intervals to ensure that revenues were appropriately tracked, expenses were valid and contractors were paid according to the contract terms. In particular, the audit focused on:

- Contractual obligations to perform reconciliations at regular intervals
- Review of the ITI analysis and oversight of the parks reconciliations for completeness and reasonability

#### **Invoicing / Reconciliation Frequency**

Park operators are awarded contracts through the contract procurement process. Contracts are awarded annually with many contracts including the option to renew for two seasons, making the total contract period up to three (3) years.

The contractors collect the park revenues for a variety of activities (varying from park to park), including but not limited to park permit sales, vehicle permit sales, kitchen shelter rentals, shower fees, and firewood sales. In addition to cash collected on site, the public can purchase park passes via the on-line reservation system (ORS). A third-party company, Outcrop, manages and maintains the ORS.

Contractors retain the revenue from the sales/rental activities and net the cash collected against their contract value. This includes cash sales collected on-site, as well as on-line sales from the ORS. Every two (2) weeks the contractors receive a cheque from Outcrop for the ORS revenue. Any monies collected above and beyond the contract value is given back to the GNWT. An example to illustrate:

A \$50,000 contract for the five (5) month park season would be valued at \$10,000/month. If during the month, the park operator collects \$7,000 in cash from park activities, they are owed \$3,000 from the GWNT. On the other hand, if the park operator collects \$12,000 in cash from park activities, they owe the GNWT \$2,000.

Throughout the contract period, contractors are required to submit invoices detailing revenues collected against the contracted amount, as outlined in the example noted above. Between regions there were inconsistencies in the frequency of invoices submitted by contractors. The table below provides a summary of our testing results regarding the frequency of invoice submission from the contractors, the frequency of the reconciliation performed by ITI park management, and the frequency of invoice payments to contractors.

Action	Frequency
<b>Invoice Submission from Contractor</b>	<ul style="list-style-type: none"> <li>■ For two (2) of the four (4) regions tested, the contractor submitted invoices monthly.</li> <li>■ For two (2) of the four (4) regions tested, the contractor submitted only one (1) invoice for the contract, at the end of the park season.</li> </ul>

<p><b>Reconciliation performed by ITI</b></p>	<p>ITI Park management reviewed and reconciled the invoices as they were received. As such:</p> <ul style="list-style-type: none"> <li>▪ For two (2) of the four (4) regions tested, the ITI Park Manager reviewed and reconciled the invoices monthly.</li> <li>▪ For two (2) of the four (4) regions tested, the ITI Park Manager reviewed and reconciled one (1) final invoice for the contract, at the end of the park season.</li> </ul>
<p><b>Invoice Payment to Contractor</b></p>	<ul style="list-style-type: none"> <li>▪ For two (2) of the four (4) regions, payments were made to the contractor on a monthly basis, for monthly outstanding balances not collected via park operations.</li> <li>▪ For two (2) of the four (4) regions, only one (1) final payment was made to the contractor at the end of the park season, for any outstanding balance not collected via park operations.</li> </ul>

**Industry Tourism and Investment (ITI) Analysis and Oversight**

The park managers are responsible to review the invoices, perform reconciliations and approve any payments made to contractors. This function was in place and there was evidence of review and approval from the park managers. However, it was noted that there was no formal, macro-level analysis of the park revenues, particularly the “other” revenues generated by the parks, such as kitchen rentals, showers, and vehicle permits, to compare revenues collected between parks and assess reasonability. ITI Finance provided a summary of revenues collected by the North and South Slave regions for the 2015 season, including “others”.

The review and reconciliation process is further complicated by other issues. Every two weeks Outcrop releases a payment to the contractors for the revenue collected via the ORS. The ITI Park Managers and Superintendents do not receive a report, or any information from Outcrop detailing the amounts paid (from Outcrop) to the contractors. This can make the reconciliation process difficult for ITI, whereby ITI Park Managers and Superintendents have to rely on the information from the contractor regarding payments received.

Finally, the ORS is meant to be used as the system to capture all revenues collected at the park. As such, the contractors are required to manually enter all of the monies collected in the park, including permit sales, kitchen rentals, shower use, and vehicle permits, and others. It was noted during interviews that many operators were not recording these revenues within ORS in a consistent manner.

**Recommendation #1:**

Overall, there are minimal controls in place to ensure the completeness and accuracy of revenues reported by park contractors. We recommend the following:

- A. All contracts require park operators to submit monthly invoices, reporting on revenues collected with complete back-up support for all revenues reported. At a minimum invoices should include the following:
  - Invoice number
  - Invoice date
  - Invoice period (what dates are covered by the invoice)
  - Detail on revenue collected, separated by revenue stream and supported by back up that reconciles to the revenue reported in the invoice
  - Invoice total

- Payment terms
- B. ITI Park Management reconciles the invoices on a monthly basis to validate that documentation is maintained to support the revenues reported.
- C. Additional controls are developed and implemented to better ensure completeness of revenue. For example, establish revenue forecasts by park and including forecasts for “other” revenues activities. To further illustrate the example, if a kitchen shelter is available for rental for the park season management could estimate that it would be rented “X”% of the time, which would represent “X” in revenues. Compare these forecasts against actual revenues reported and follow-up on major discrepancies.

**Management Response to Recommendation #1:**

Action Plan	Completion Date
<p>A. Starting in April 2016, RFPs for the new Park Operator contracts include a description of invoice requirements. This includes separate reporting of revenue and required back up. For contracts that were already in place, Management explained the requirements to each contractor. Management will send the Regional Park Managers the requirement for invoices i.e. invoice number, invoice date, invoice total and payment terms.</p> <p>B. Starting in April 2016, there was a change in the reporting process whereby revenue is separately reported and reconciled. Contractors provide deposits to ITI separate from their invoices and include the back up with these deposits. (Issue Closed.)</p> <p>C. ITI is establishing site visits by ITI staff to compare occupancy reports to actual visitors to determine if reservations in the system are complete. (Manager of parks for each region will review completed reports to see if review is effective - August 31, 2016)</p>	<p>A. August 31, 2016 B. Issue Closed C. August 31, 2016</p>

**2.3.2 Reliability and Integrity of Information**

The audit examined if access controls related to the Online Reservation System (ORS) had appropriate segregation of duties (SOD), were documented, communicated, and were reliable. Specifically, the audit validated:

- User access was documented, reasonable and appropriate for the role.
- Segregation of duties were in place.
- Information in the Online Reservation System was accurate and reliable.

**System Access and Segregation of Duties**

The walkthrough performed with Outcrop staff validated that the Park Contractors access to the ORS is reasonable and appropriately segregated. Contractors only have access to the park they operate and they do not have write access in the system.

However, it was noted that formal documentation prescribing user access by role is not in place. Outcrop provides access to users via verbal and/or email requests from ITI. Based on interview discussions it was not clear who the ITI point of contact is to determine and approve access to the ORS, and communicate with Outcrop. As such, actual access in the system could not be compared to documented user access requirements, by role.

**ORS Accuracy and Reliability:**

To validate the accuracy of the revenues, reservations and reports captured by the ORS, the audit included a walkthrough of the reservation, refund and reporting process. To complete this test, the following steps were performed:

- 1) A dummy reservation was entered into the system
- 2) A finance report was run, capturing the revenue from the reservation
- 3) The dummy reservation was refunded
- 4) A finance report was run, capturing the refund (90% refund, 10% revenue remaining for cancellation fee)

The results of the walkthrough indicated that the revenue from the sale and the refund was accurately recorded, with one exception. The final finance report, showing both the revenue and the refund did not net the amounts (revenue positive, refund negative). Instead the numbers were added together, totalling an incorrect number. To illustrate:

- 1) Revenue from dummy reservation: \$100
- 2) Finance report capturing revenue: \$100
- 3) Refund performed: \$90
- 4) Finance report capturing refund: \$190 (revenue should net to \$10 instead of \$190)

Outcrop stated that this was a glitch in the system which they are aware of and are working on correcting before the season opens.

**Recommendation #2:**

We recommend that:

- A. ITI leverage their internal IT department to liaise with Outcrop and ITI Management to provide some IT oversight and expertise regarding the ORS.
- B. Management develop a user access listing prescribing the functionality and access required by role. Access levels should be periodically reviewed.
- C. Management conduct a review of historical data to ensure that that the system “glitch” found has not impacted payments made to contractors. Additionally, management should confirm with Outcrop that the system “glitch” has been addressed.

**Management Response to Recommendation #2:**

Action Plan	Completion Date
A. Ongoing discussions exist between the Director, Tourism and Parks and the Office of the Chief Information Officer and Informatics Shared Services since the inception of the Online Reservation System in 2014.	A. Not Specified B. August 31 2016 C. Issue Closed

<p>(On going). "Transform ICT" project may impact the online reservation system.</p> <p>B. ITI will complete user access manual and review procedures (August 31 2016 – Director Tourism and Parks)</p> <p>C. Review for 2015 was completed in April 2016 based on significant differences (&gt;\$1000 per park) and determined no payment owed to operator. (Issue Closed).</p>	
--	--

### **2.3.3 Compliance**

There are multiple legislations and regulations in place with respect to contracting, finance, and operations of the Territorial Parks. The audit focused on the following:

- Financial Administration Manual (FAM)
- Territorial Parks Act
- Workers Safety and Compensation Commission (WSCC) Regulations
- Emergency Protocols

Additionally, the audit performed testing to review the quality of the invoices submitted by the contracted park operators with respect to accuracy, completeness and timeliness.

#### **Financial Administration Manual (FAM)**

The FAM was developed for public officers with financial signing responsibility in Government departments and contains legislation, regulation, and financial administration policy. Several key, relevant sections of the FAM were selected for testing. For example, FAM requires the following with respect to 3<sup>rd</sup> parties collecting revenue on behalf of the government:

FAM reference	FAM requirement
4.2.2	A contract with a revenue agent must set out the required frequency for remitting and reporting revenue, e.g., daily, weekly, monthly or annually. The contract must also specify the method for remitting, e.g., direct bank deposit, electronic fund transfer, remittance by-hand to a Government office, or mail
4.2.4	A revenue agent, who does not have daily access to a bank or Government office and who collects or receives revenue estimated to exceed \$10,000 per year, shall remit and report revenue weekly by mail. The revenue agent shall provide security equivalent to the estimated average remittance for two weeks of the active sale season, through bonding, cash deposit, or letter of irrevocable guarantee from a bank.
4.2.6	Any costs of revenue collection, (e.g., debit and credit card fees and service charges for nonnegotiable cheques, and any loss of revenue due to fraud, theft, negligence or casualty) must be carried by the revenue agent and may not be deducted from revenue remitted to the Government.



Aside from section 3400 – *Contract Registry*, which was found to be fully compliant with FAM requirements, the other FAM criteria selected were not able to be tested. (See appendix B for a listing of FAM requirements selected for testing). It was found that the FAM requirements related to revenue collected at the Parks were not being adhered to. The contractors collect all revenues generated through park operations and then net the revenues from the total contract value. As such, the revenues collected by the contractors have been classified by ITI as the contractor's revenue. The audit did not identify any evidence of approval or authority for the system of netting revenues and FAM exemption.

### **Territorial Parks Act**

The Territorial Parks Act include the specific regulations that the Territorial Parks must abide by, including specific operational-level requirements. During the interview process, Park Managers and Superintendents stated that Park Officers visit the parks regularly (weekly / bi-weekly depending on the park location) to inspect the park and validate that the requirements identified in the Act are being adhered to. This visit and inspection is evidenced by the completion of a Park Inspection Form.

As such, a sample of park inspection forms were requested, representing all nineteen (19) parks in scope. They were reviewed for evidence of the Park Officer's assessment of compliance to the key requirements of the Territorial Park Act. Three (3) of the nineteen (19) parks did not provide any park inspection forms. The remaining sixteen (16) parks did provide a number of forms, suggesting that park inspections were occurring regularly and were documented.

The forms varied in format, some were checklists with a five-point rating scale on a variety of elements of the park, while others were blank sheets where officers provided their comments in narrative form. The majority of the park inspection forms included sign off from the park officer who completed the inspection and the contractor. However, the park inspection forms did not include evidence to suggest that any of the key requirements found within the Territorial Park Act (i.e. required quiet time, vehicles/trailers parked in designated areas, adherence to fire requirements, and review of permits issued) are being reviewed and assessed during the inspection.

Finally, a walk-through was performed at three (3) territorial parks (Prelude Lake, Fred Henne and Fort Simpson) to validate that signage was displayed in both official languages. Of those three (3) parks, one (1) (Fred Henne) displayed some signage in both English and French, and one (1) Fort Simpson displayed some graphic signage, that did not require the use of words. However, for all three (3) parks visited the majority of the signage viewed was in English only.

### **WSCC Regulations**

A new regulation has been put into effect in June 2015 from the Workers' Safety & Compensation Commission (WSCC), regarding Occupational Health and Safety (OHS). The regulation indicates that GNWT is responsible for the safety of the park contractors as well as any employees employed by park contractors. Interviews conducted with ITI Park Management and Regional Superintendents stated that these new regulations have not yet been implemented. Meaning the processes surrounding the requirements for contractors to track safety, training, and inspections of parks, related to health and safety of employees, have not been developed, formalized or communicated to the contractors to date.

### **Emergency Protocols**

In terms of emergency protocols, good practices were observed related to the documentation and communication of emergency protocols for a number of the regions. Detailed response plans, including contact information and step-by-step instructions on dealing with emergencies were observed for three (3) of the four (4) regions; Deh Cho and North Slave and South Slave.

However, no documentation related to emergency protocols was provided from the Inuvik region and the Manager of Parks stated that formal emergency protocols are not in place other than an emergency contact listing.

### **Quality of Invoices**

A total sample of eight (8) park invoices submitted by park contractors were requested for testing. This sample represented parks from all four (4) regions; North Slave, South Slave, Deh Cho and Beaufort Delta. It was expected that the invoices would be submitted monthly and would include:

- Total contract value for the period.
- Total revenues collected for the period.
- Complete back-up support for all revenues collected, which reconciled to the revenue totals reported in the invoice.

Key findings from the reconciliation testing results included:

- For six (6) of the eight (8) contractor invoices tested there was insufficient support to validate the revenues reported. Examples include missing documentation to support the amount of ORS revenue collected and revenues collected for park permits at the gate.
- For six (6) of the eight (8) contractor invoices tested, the supporting documentation provided did not fully reconcile to the revenues reported due to a number of issues, including; lack of supporting documentation to complete the reconciliation, supporting documentation provided did not match reported revenue, and calculation errors.
- For two (2) of the eight (8) contractor invoices tested, contractors were over-paid according to the parameters of the original contract. In one instance the contractor was over-paid by \$5,122. An informal agreement was hand-written on the reconciliation (and signed by the contractor and the Parks Manager) that in the spring the contractor would return to the park and complete brushing services valued at \$4,895 (per the handwritten contract). In the second instance, the contractor received an additional \$21,250 in payment in excess of the contracted amount. The payment noted that there had been more park visitors that year, which warranted the increase in contract amount. However, no formal documentation was provided, such as a contract amendment, or formal approval.

### **Recommendation # 3:**

We recommend that:

- A. The “revenue netting” process is reviewed and a formal decision to continue or discontinue this process is confirmed. Additionally, we recommend that the FAM requirements relevant to the operations of the territorial parks (including sections 4.2.2, 4.2.4, and 4.2.6) are identified, and processes compliant with the FAM requirements are set up, clearly communicated to park contractors, and are included in the contracts, where applicable.
- B. The WSCC requirements relevant to the park operations are identified and that processes are communicated to and implemented by the park contractors in compliance with the regulations.
- C. Park inspections be completed and documented at regular intervals.
- D. Park inspection forms be updated to include evidence of review of the key Territorial Park Act Regulatory requirements.

- E. The park signage be updated and include the use of graphic and symbolic signage, similar to some of the signage currently used in Fort Simpson.
- F. Payments made to park operators are in-line with the contract amounts. If additional payments are required, a formal contract amendment is procured and approved. (See recommendation 1 for additional recommendations related to the invoicing process)
- G. Emergency protocol procedures are updated to be consistent in all four (4) regions.

**Management Response to Recommendation #3:**

Action Plan	Completion Date
<p>A. Prior to this audit, ITI had made the decision to remove the ‘netting’ of revenue from the invoices for the 2016 summer season. Processes have been completed with input from the Department of Finance and final review to be completed by the Department of Finance for the collection of revenue. Management to ensure that these processes are communicated to the Operators (July 31, 2016, Regional Superintendents). Final procedures to be signed off by the Department of Finance (August 31, 2016, Director of Finance).</p> <p>B. ITI has an obligation to identify hazards but not responsible for the safety of the contractor’s employees. New safety requirements were included in the contract and the Park Safety Plan has been completed and distributed electronically. This includes templates for hazard identification. (Issue Closed)</p> <p>C/D. Park inspections are ongoing and documented. The park inspections (the ones reviewed in this audit) include documentation on the Operator’s performance in keeping washrooms clean and in good repair for example. Inspections related to items in the Territorial Park Act were included in the Park Officer checklist. ITI has created an incident database whereby the Officer will enter an incident and it will be escalated as appropriate. This will not require the incident to be documented on paper but rather as it happens in real time. There is also a Parks Officer Manual that outlines what Officers should be reviewing. Prior to this audit a process to prepare weekly reports from each Region for the Assistant Deputy Minister was established and will continue to exist. (Director of Tourism and Parks to review process at end of season to ensure database and weekly reporting is appropriate -October 31, 2016)</p> <p>E. ITI has been updating signage for French language as budget permits and will continue to do so. When possible, symbols will be used (March 31, 2018, Director of Policy Legislation and Communications and Director, Tourism and Parks).</p>	<ul style="list-style-type: none"> <li>A. August 31, 2016</li> <li>B. Issue Closed</li> <li>C. October 31, 2016</li> <li>D. October 31, 2016</li> <li>E. March 31, 2018,</li> <li>F. Issue Closed</li> <li>G. September 30, 2016</li> </ul>

<p>F. Effective April 2016, under the new process for reporting revenue separately from the contractor's invoice, the risk has been mitigated. (Issue Closed)</p>	
<p>G. Inuvik Emergency plan to be completed. (September 30, 2016 – Superintendent Inuvik).</p>	

**2.3.4 Asset Safety**

The audit included review of the physical inspection and maintenance of park assets, as well as the tracking of and accounting for assets.

**Park Inspection Forms – Assets**

Assets are monitored through periodic park inspections. As part of the periodic park inspections, park management is required to account for and capture the condition of park assets.

As previously noted, park inspection forms were requested for all nineteen (19) parks in scope, with forms provided for sixteen (16) of the nineteen (19) parks.

The audit found that all sixteen (16) park inspection forms provided included evidence of asset review.

**Accounting for Assets**

Within the System for Accountability and Management (SAM) Finance module there is a sub-module for assets, which is where the asset listing is maintained. Only designated individuals in the Finance and Risk Management and Insurance departments have access to add, delete and edit the listing.

Assets are broken into two (2) categories:

- 1) Capital assets over \$50,000; SAM submodule maintained by the Finance group.
- 2) Non-capital assets - under \$50,000; SAM submodule maintained by the Risk Management and Insurance group.

Adding and/or deleting assets to the listing in SAM requires completion of a form. This is completed by the regional superintendent or manager of parks. The form is then sent to the Director of Finance ITI, who sends the request to the Financial Reporting, or Risk Management and Insurance group, who approves and enters/deletes/ edits the asset.

Quarterly, the Director ITI Finance reviews access to the SAM, including the asset listing, makes any changes required and formally signs off on the access. There is no document prescribing access by role, and as such the access is left to the discretion of the Director. During the meeting the Director provided evidence of the Jan 2016 access review and the Oct 2015 access review (the last two quarters).

Annually, as part of the year end process, the Director of Finance ITI conducts a review of the assets to ensure that the listing is complete and up to date. She sends a listing of the regional assets (both capital and non-capital) to the regional superintendents. They review the listings and complete the paperwork to add/delete any assets. The forms are sent to the Director of Finance ITI, who reviews the request and sends it to Financial Reporting, or the Risk Management and Insurance group, for updating in SAM.

**2.3.5 Efficiency and Effectiveness**

The audit assessed the nineteen (19) Territorial Park contracts, representing all parks operated by independent contractors, to determine if the contracting terms and conditions and general contracting practices were in-line with public sector practices.

The audit identified the following good practices:

- All contracts were signed by both parties.
- Contracts included a summary description of services to be provided, including sanitary and site maintenance schedules.
- Terms of payment were communicated (i.e. terms for making payments to the contractors).
- The contracts required a clear document retention period of 3 years (7 years for newer contracts)

The audit identified the following opportunities for improvement:

- **Invoicing:** The contracts did not specify the templates, format to be used, and back-up support that should be provided to support the invoice.
- **Online Reservation System (ORS):** The ORS is meant to capture all revenues collected by the Contractors; including online payments made directly through the ORS, and revenues collected at the gate for permits, kitchen rentals, etc. The requirement for revenues to be input into the ORS in a timely could be included in the contract, along with required timelines and regular reporting requirements.
- **Regulatory Compliance:** The contracts did not include requirements or procedures to ensure that the contractors are in compliance with the new occupational health and safety (OHS) regulations established in June 1st, 2015 by the Workers Safety and Compensation Committee (WSCC). Additionally, FAM requirements and procedures have not been documented or included in the park contracts.

In addition to our review of the contracts, interviews with ITI Park Superintendents identified that at times the legal nature of the contract language creates obstacles for contracts in terms of comprehension.

**Recommendation #4:**

We recommend that management update their standard terms and conditions within their contracts to include:

- A. Clear invoicing requirements that include billing procedures, frequency of reporting, templates to be used, back-up support to be provided.
- B. Requirements to update the ORS on a regular, timely basis.
- C. See recommendation #3 for regulatory requirement updates.
- D. We recommend that Park Contracts be written in plain language to improve comprehension of the contract terms.

**Management Response to Recommendation #4:**

Action Plan	Completion Date
A/B Requirement for invoicing and revenue reported included in new RFPs in 2016. For contracts that were a renewal in 2016, Management has communicated the new requirements. Currently system able to capture camping permits and vehicle permits. Other revenue is tracked separately. System changes to expand the functionality of	A/B - April 30, 2017 C - February 28, 2017 D - July 31, 2016



the system for all revenues will be given consideration in the next cycle (Director of Finance, Director Tourism and Parks, April 30, 2017).

C. Starting in 2016, new WSCC requirements for contractors to have a written safety plans was included in the contract. ITI to add specific FAM references for revenue in the contracts for 2017 (Director of Finance February 28, 2017).

D. Suggestion has been sent to Procurements Shared Services February 4, 2016. Contracts in the GNWT are a standard template and reviewed by the Department of Justice. For operators who are not as conversant with English, the Superintendent of each Region will ensure the operators understand their requirements of the contract. (July 31, 2016 – Applicable Superintendents).

## APPENDIX A – AUDIT CRITERIA

Based on the risk assessment completed, planning interviews and document review, the following audit criteria were developed to support the audit objective, these were approved within the audit work plan.

Audit Area	Audit Criteria
<b>1. Governance Framework</b>	<p>1.1 Reconciliations are performed at regular intervals to ensure that revenues are appropriately tracked, expenses are valid and contractors are paid according to the contract terms.</p> <p>1.2 Formal contract oversight activities are performed to ensure that the quality of service delivered by contractors meets the contractual requirements.</p>
<b>2. Reliability and Integrity of Information</b>	<p>2.1 Access controls related to the Online Reservation System (ORS) support appropriate segregation of duties and are documented, communicated and in place</p> <p>2.2 Data and reports obtained from the online reservation system are reliable</p>
<b>3. Compliance</b>	<p>3.1 GNWT is compliant with the key regulatory and legislated requirements included in the Financial Administration Manual (FAM) and the Parks Act.</p>
<b>4. Assets and Visitor Safety</b>	<p>4.1 Park inspections formally include review of and reporting on GNWT assets, and are conducted at regular intervals.</p> <p>4.2 Capital and non-capital assets are properly tracked and accounted for.</p> <p>4.3 Emergency procedures are in place to provide park operators and guests with clear protocols to follow should an emergency situation arise.</p>
<b>Efficiency and Effectiveness</b>	<p>5.1 Contracting terms are complete, and in line with contracting best practices</p> <p>5.2 Contracting “Operational” Terms are complete and in line with operational best practices.</p>

## APPENDIX B –FAM REQUIREMENTS

The following sections of the *Financial Administration Manual* were originally included in our review:

### 3401 Registry and Reporting System

Relevant Section	Regulation
3.1	In accordance with the following Directives, the Minister of ITI is responsible to collect competitive and non-competitive procurement information, data and change orders required to administer and support the GNWT Contract Registry and Reporting System.
4.1	<p>The Contract Registry shall include information on each contract over \$5,000 that is to be competitively and non-competitively awarded by the GNWT, (including multi-year contractual arrangements, regardless of the year initiated, as defined in Section 44(2) of the Financial Administration Act) and will be incorporated into resulting contract reports.</p> <p>Each Department/Agency will designate a representative to collect and provide procurement information, data and change order(s) to the BIP Monitoring Office, ITI. The Departmental/Agency Representatives will be required to complete and submit the following standard documents, where applicable:</p> <ol style="list-style-type: none"> <li>1. Competitive contracts;</li> <li>2. Non-competitive contracts;</li> <li>3. Evaluation and Award Results;</li> <li>4. Summary of Change Order(s).</li> </ol>
4.2.1	<p>The GNWT contracts over \$5,000 Report will provide information by fiscal year in two formats:</p> <p>1) Detailed Report by Department / Agency:</p> <ul style="list-style-type: none"> <li>• Contract Number;</li> <li>• Contract Title;</li> <li>• Contract Designation (Goods; Services);</li> <li>• Construction;</li> <li>• Description of Contract Designation;</li> <li>• Contract Type (Tender, Proposal, Negotiated, Sole Source, SOA);</li> <li>• Description of Contract Type;</li> <li>• Business Name;</li> <li>• Business Community;</li> <li>• Business Status (BIP Registered, NWT Non-BIP, Not in NWT);</li> <li>• Contract Amount;</li> <li>• Total Contract Amount (including Change Orders).</li> </ul> <p>2) Summary Report:</p>



	<ul style="list-style-type: none"> <li>• Contract Designation (Goods, Services);</li> <li>• Construction;</li> <li>• Description of Contract Designation;</li> <li>• Contract Type (Tender, Proposal, Negotiated, Sole Source, SOA);</li> <li>• Description of Contract Type;</li> <li>• Business Name;</li> <li>• Business Status (BIP Registered, NWT Non-BIP, Not in NWT);</li> <li>• Total BIP Bid Adjustments (NWT Content, Local Content, BIP Premium);</li> <li>• Total Number of Contracts;</li> <li>• Total Contract Amounts (including Change Orders).</li> </ul>
5.1	The ITI should provide training to departmental representatives to enable them to provide the information required for the GNWT Contract Registry and Reporting System.

### 2904 Deposit Public Money

Relevant Section	Regulation
4.3.1	<p>Departments shall:</p> <ol style="list-style-type: none"> <li>1. Safeguard in locked facilities any monies held overnight;</li> <li>2. Limit custody of money and access to locked facilities to authorized cashiers and supervisors;</li> <li>3. Change vault combinations whenever an employee with knowledge of the combination leaves his or her position; and,</li> <li>4. Change vault combinations at least once a year in any case.</li> </ol>
4.4.2	<p>Receipts exceeding \$500 in total must be deposited the same day. Smaller amounts must be deposited at least on a weekly basis:</p> <ol style="list-style-type: none"> <li>1. in the Consolidated Revenue Fund;</li> <li>2. in a revenue transfer account;</li> <li>3. by mail to a regional or headquarters FMBS office via internal mail or Canada Post, whichever is quicker; or,</li> <li>4. by courier, if appropriate.</li> </ol> <p>Deposits by mail or courier must be made under dual control. All money and accompanying documents must be sent in a locked bag designed for the purpose. Only the receiving office may have a duplicate key. The container must be opened in the presence of two officers responsible for deposit who shall verify the amount and sign the Daily Register of Incoming Revenue (DRIR).</p>
4.4.3	All receipts for deposit must be recorded on a daily basis in SAM.
4.6.4	No further recovery action is to be performed, beyond those automatically generated by SAM, when the total owed by a customer is \$25 or less. If no additional business is anticipated with this customer, the amount is to be written off.

### 3561 Revenue Agency Contracts

Relevant Section	Regulation
4.2.6	Any costs of revenue collection, (e.g., debit and credit card fees and service charges for nonnegotiable cheques, and any loss of revenue due to fraud, theft, negligence or casualty) must be carried by the revenue agent and may not be deducted from revenue remitted to the Government.
4.1.3	Every class of contracts (or any non-standard contract) with an exclusive revenue agent must be approved in advance by the Comptroller General and the Legal Division of the Department of Justice unless the contract relates to a special event, in which case it shall be subject to the conditions specified in FAM 2812.
4.2.2	A contract with a revenue agent must set out the required frequency for remitting and reporting revenue, e.g., daily, weekly, monthly or annually. The contract must also specify the method for remitting, e.g., direct bank deposit, electronic fund transfer, remittance by-hand to a Government office, or mail
4.2.4	A revenue agent, who does not have daily access to a bank or Government office and who collects or receives revenue estimated to exceed \$10,000 per year, shall remit and report revenue weekly by mail. The revenue agent shall provide security equivalent to the estimated average remittance for two weeks of the active sale season, through bonding, cash deposit, or letter of irrevocable guarantee from a bank.

### 1802 Approval Authorities

Relevant Section	Regulation
4.3.2	Accounting Officers are responsible for expenditure and disbursement control matters consistent with sections 44(1)(b), 48 and 49(2)(b) of the FAA , including: <ol style="list-style-type: none"> <li>1. Performing adequate sampling tests (see Appendix B) to assess the quality of the review at the primary level of responsibility;</li> <li>2. Reviewing and verifying the voucher documentation before any payment is made (see Appendix D for checklist);</li> <li>3. Ensuring compliance with all applicable legislation, policies and directives;</li> <li>4. Authorization is provided electronically in the System for Accountability and Management and in writing.</li> </ol>
4.4.2	A Revenue Officer must provide proper certification before public money is taken into possession and under control of the Government. The certification includes: <ol style="list-style-type: none"> <li>1. Account verification;</li> <li>2. Issuance of a receipt;</li> <li>3. Proper recording of the revenue.</li> </ol>

## APPENDIX C – FINDINGS RATING SCALE

Our findings are classified and prioritized according to the following risk-ranking methodology<sup>1</sup>:

Risk Ranking	Description
<b>4. Extreme</b>	Occurrence would have extreme impacts on stakeholders at the Government of Northwest Territories and, Existing controls are inadequate or non-existent, suggesting that this risk is almost certain to materialize
<b>3. High</b>	Inability or significantly reduced ability to achieve expected results and organizational priorities, and Existing controls are very weak, suggesting that this risk is likely to materialize
<b>2. Moderate</b>	Moderate impact on ability to achieve business objectives, and Existing controls are generally adequate (few significant weaknesses) suggesting that this risk is only moderately likely to materialize
<b>1. Minor</b>	Limited impact on ability to achieve expected results and organizational priorities, and There are minor weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize
<b>1. Insignificant</b>	There is little to no impact on the ability to achieve expected results and organizational priorities, and There are no significant weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize

<sup>1</sup> The risk-ranking methodology is the same risk-ranking methodology used by the Government of Northwest Territories Internal Audit Bureau