



MAY 09 2018

**CONFIDENTIAL**

File: 7820-20-GNWT-151-131

DR. JOE DRAGON  
DEPUTY MINISTER  
ENVIRONMENT AND NATURAL RESOURCES

**Access to Information and Protection of Privacy Assessment**

Enclosed is the above referenced Assessment.

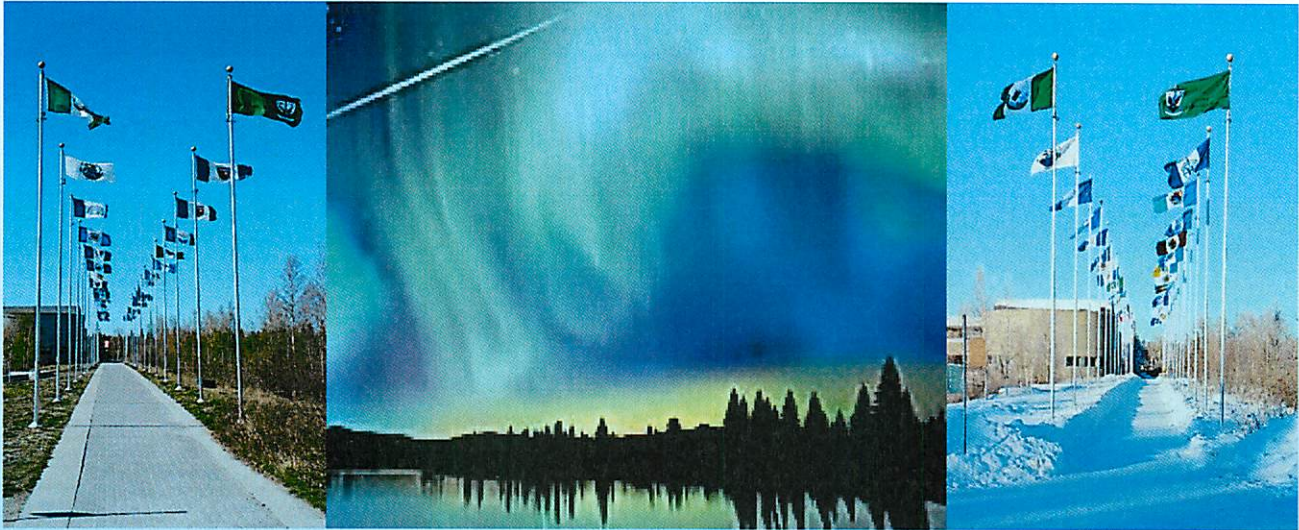
We will schedule a follow-up in the future to determine the progress of the agreed upon Management Action Plan. However, we would appreciate an update by August 2018 on the status of the management action plan.

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. Hilda Balsillie, A/Director, Finance and Administration, ENR



# ENVIRONMENT AND NATURAL RESOURCES

## Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



## **ENVIRONMENT AND NATURAL RESOURCES**

### **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

DR. JOE DRAGON  
DEPUTY MINISTER  
ENVIRONMENT AND NATURAL RESOURCES

**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 Environment and Natural Resources 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 to 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 Environment and Natural Resources, 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 “ad-hoc”, meaning that the processes were primarily dependent on the individuals getting things done. The immediate task for the department was to develop systematic privacy processes and then focus on documenting 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
- Individuals providing personal information to ENR be advised of their privacy rights.

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	ENR				
	Low					
	Very Low					
		Not Compliant	Partially Compliant	Compliant	Fully Compliant	Perfectly Compliant
		<b>Compliance Classification</b>				



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 ENVIRONMENT AND NATURAL RESOURCES

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

### Scope and Objectives

The Government of the Northwest Territories (GNWT) issued a request for proposal, for an operational audit reviewing departmental compliance with Part 2 of the ACCESS to Information and Protection of Privacy Act (ATIPP or “the Act”). Crowe MacKay LLP (Crowe MacKay), being the successful proponent. 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 Environment and Natural Resources (“ENR”) meets its responsibilities through programs it offers through its divisions of:

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

ENR collects personal information through:

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

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



# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

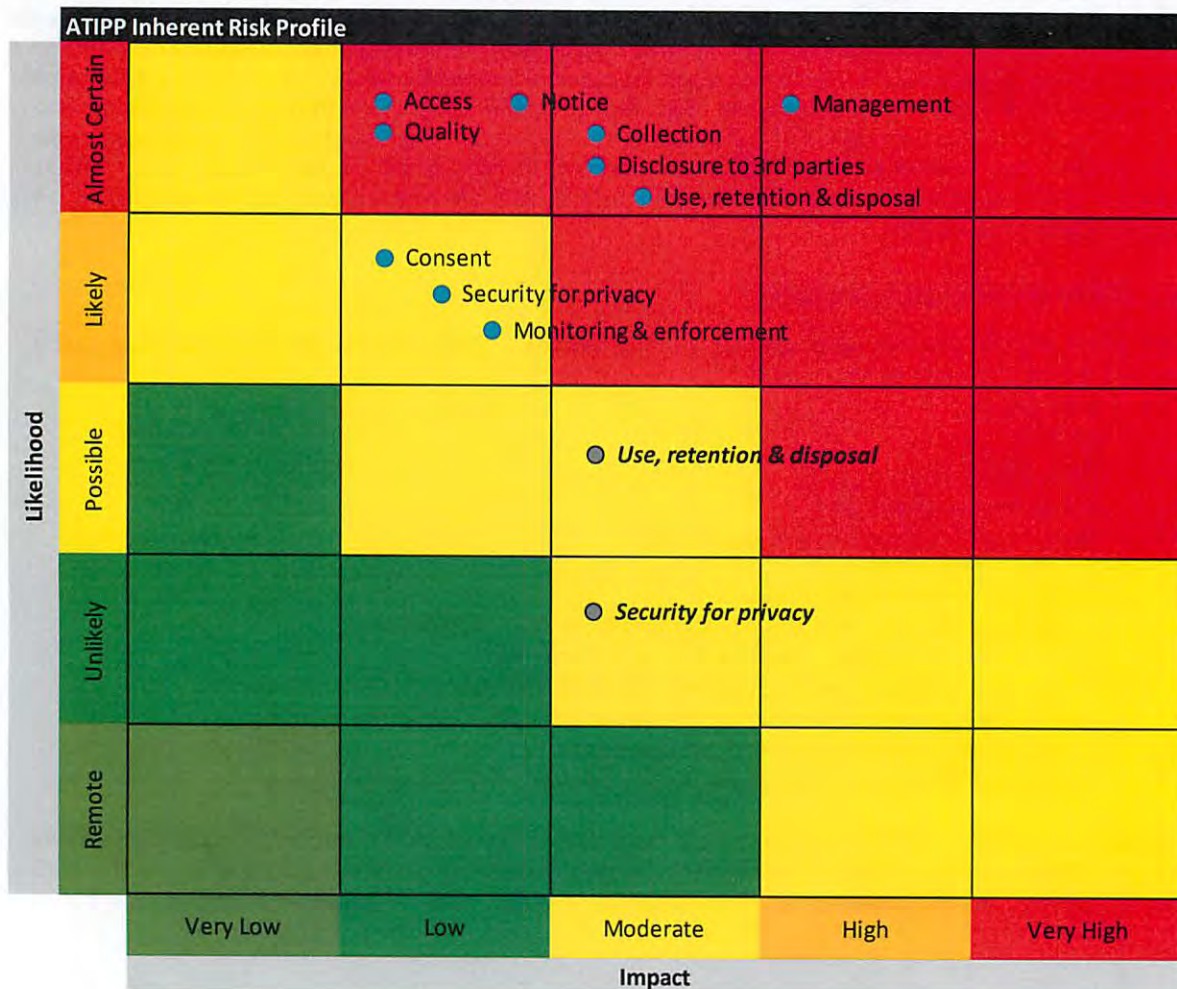
## ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

### Overview

### Risk Profile

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

### RISK HEATMAP



# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Compliance with ATIPP Part 2 Protection of Privacy

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

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

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

### Maturity Rating against Privacy Maturity Model

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

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

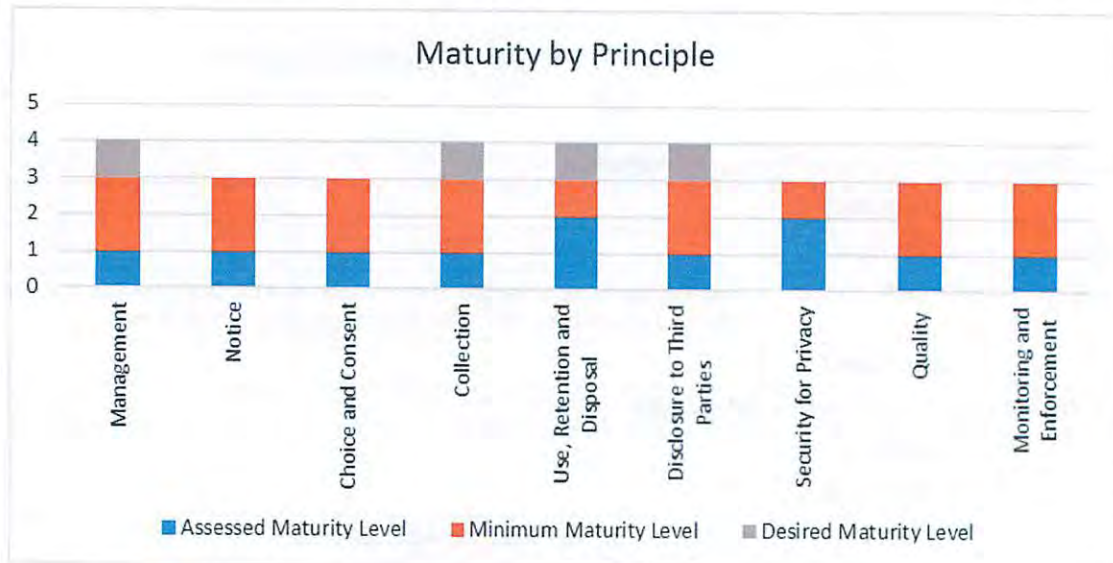
**Minimum Maturity Level** – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

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

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



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

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

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
<p><b>Notice</b></p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address notice to individuals.</li> <li>Notice is not provided on all forms used to collect personal information.</li> </ul> <p><i>See observation 3.</i></p>
<p><b>Consent</b></p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address consent of individuals.</li> <li>Implicit consent is obtained on personal information collection forms.</li> <li>Explicit consent is obtained on information collection forms.</li> <li>Consent is not documented when information is collected verbally.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Collection</b></p> <p>The department collects personal information only for the purposes identified in the notice</p>	Ad Hoc	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address collection of personal information.</li> <li>The type of personal information collected and the method of collection for personal information collected by forms is known to the individual and the department discloses the collection of information through the use of cookies.</li> <li>Notice of collection is not documented when information is collected verbally.</li> <li>Methods and forms of collecting information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.</li> <li>A formal procedure/process does not exist to ensure only information needed is collected.</li> </ul> <p><i>See observation 4.</i></p>
<p><b>Use, retention and disposal</b></p> <p>The department limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.</p>	Repeatable	<ul style="list-style-type: none"> <li>A privacy policy has not been formally designed and documented to address use, retention and disposal.</li> <li>A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for.</li> <li>Retention and disposal of information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the Digital Integrated Information</li> </ul>

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>Management System (DIIMs) which allows for information to be retained for no longer than necessary and is disposed of at that time.</p> <p><i>See observation 5.</i></p>
<p><b>Disclosure to third parties</b></p> <p>The department discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be taken if the information was misused by the third party.</li> <li>• Information sharing agreements do not exist with other departments to provide instructions or requirements to the departments regarding the personal information disclosed, to ensure the information is only used for the purpose for which it was collected and to ensure the information will be protected in a manner consistent the department's requirements.</li> </ul> <p><i>See observation 6.</i></p>
<p><b>Security for privacy</b></p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address security for privacy. The department has a security program in place to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction however the program is not formally documented.</li> <li>• Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place by the Informatics Shared Services Centre.</li> <li>• Physical access to personal information is restricted through access to building, floor restriction access, storage in secure and locked cabinets.</li> <li>• Security measures exist over the transmission of data but are not formally designed and documented.</li> <li>• Tests of all safeguards in place are not performed.</li> </ul> <p><i>See observation 1.</i></p>
<p><b>Quality</b></p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Ad Hoc	<ul style="list-style-type: none"> <li>• A privacy policy has not been formally designed and documented to address quality to ensure personal information is complete and accurate for the purposes for which it is to be used and it is relevant to the purposes for which it is to be used.</li> </ul>

## DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

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

## Observations and Recommendations

### Observation 1

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

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

#### Management Response:

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

### Observation 2

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

## DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

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

#### Management Response:

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

### Observation 3

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

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

#### Risk Profile:

Risk Impact	Lack of notice on the forms will result in the department not being compliant with ATIPP legislation.
Risk Responsibility	Director

## DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

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

#### Recommendations:

We recommend that:

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

#### Management Response:

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

#### Observation 4

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

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

#### Management Response:

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



## DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

assessment tool is under development by the Dept. of Justice and ENR will comply with any procedures/policies as dictated by the Dept. of Justice to its enactment.	
---	--

#### Observation 5

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

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

#### Management Response:

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

# DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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

### Observation 6

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

- A listing of all information provided to other departments be compiled which details what information is provided, to which department and for what use and that the listing be reviewed to assess whether the information shared is required to be shared.
- Information sharing agreements be entered into with departments that receive necessary personal information from ENR and that the agreements provide instructions or requirements regarding the personal information disclosed to ensure the information is only used for the purpose for which it was collected and to ensure the information will be protected in a manner consistent the department's requirements.

#### Management Response:

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

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

# 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 Federer

Philip M. Juravel, CPA, CITP

Sagi Leizerov, Ph.D., CIPP

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

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

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

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

### ***Staff Contacts:***

Nicholas F. Cheung, CA, CIPP/C

CICA

Principal, Guidance and Support

and

Nancy A. Cohen, CPA, CITP, CIPP

AICPA

Senior Technical Manager, Specialized Communities and Practice Management

## 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**

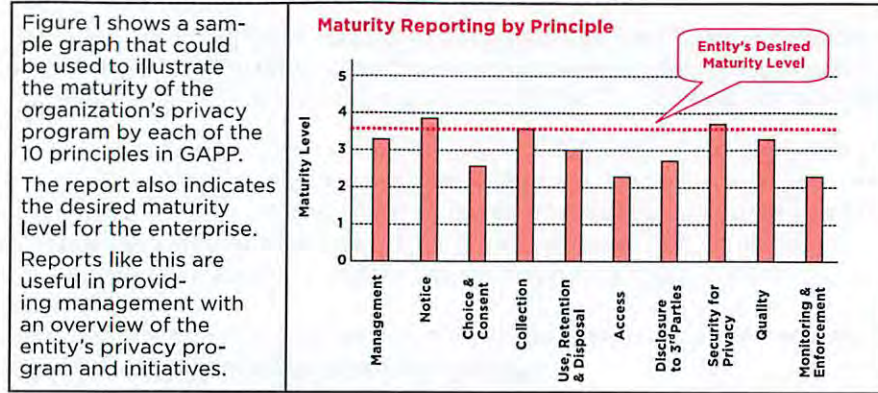
The PMM can be used as the basis for reporting on the status of the entity's privacy program and initiatives. It provides a means of reporting status and, if assessed over time, reporting progress made.

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.

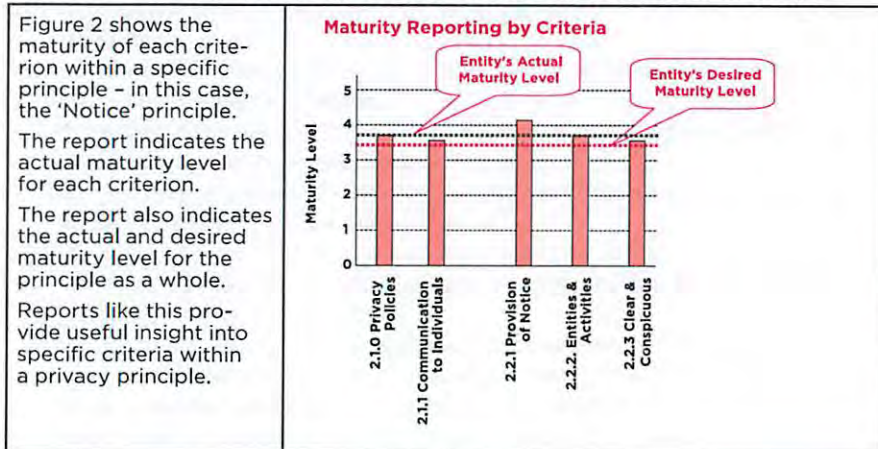
Privacy maturity reports can be in narrative form; a more visual form can be developed using graphs and charts to indicate the level of maturity at the principle or criterion level.

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

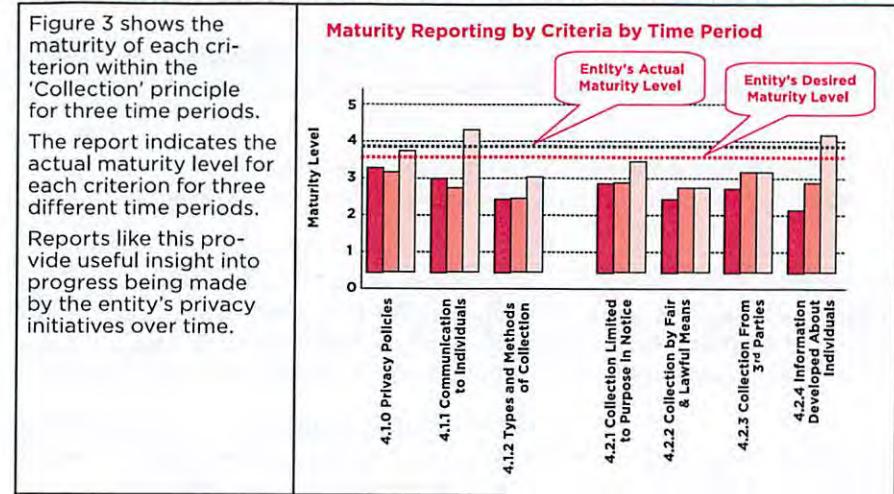
**Figure 1 – Privacy Maturity Report by GAPP Principle**



**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>	Changes in business and regulatory environments are addressed sporadically in any privacy initiatives the entity may contemplate. Any privacy-related issues or concerns that are identified only occur in an informal manner.	The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented.	The entity has implemented policies and procedures designed to monitor and act upon changes in the business and/or regulatory environment. The procedures are inclusive and employees receive training in their use as part of an enterprise-wide privacy program.	The entity has established a process to monitor the privacy environment and identify items that may impact its privacy program. Changes are considered in terms of the entity's legal, contracting, business, human resources and technology.	The entity has established a process to continually monitor and update any privacy obligations that may arise from changes to legislation, regulations, industry-specific requirements and business practices.
<b>NOTICE (5 criteria)</b>	<b>The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.</b>					
<b>Privacy Policies (2.1.0)</b>	The entity's privacy policies address providing notice to individuals.	Notice policies and procedures exist informally.	Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented.	Notice provisions in privacy policies cover all relevant aspects and are fully documented.	Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.	Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance.
<b>Communication to Individuals (2.1.1)</b>	<p>Notice is provided to individuals regarding the following privacy policies: purpose; choice/consent; collection; use/retention/disposal; access; disclosure to third parties; security for privacy; quality; and monitoring/enforcement.</p> <p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>	Notice to individuals is not provided in a consistent manner and may not include all aspects of privacy, such as purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding some of the following privacy policies at or before the time of collection: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Notice is provided to individuals regarding all of the following privacy policies at or before collection and is documented: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement.	Privacy policies describe the consequences, if any, of not providing the requested information and indicate that certain information may be developed about individuals, such as buying patterns, or collected from other sources.	Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.

## Appendix A

AICPA/CICA Privacy Maturity Model

GAPP - 73		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.

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



# Appendix A

AICPA/CICA Privacy Maturity Model

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

## Appendix A

AICPA/CICA Privacy Maturity Model

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

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

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.

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 and recognize the consequences of violations of security policies and procedures. Where portable devices are used, only authorized and registered devices such as portable flash drives that require encryption are permitted. Use of unregistered and unencrypted portable devices is not allowed in the entity's computing environment.	Management monitors new technologies to enhance the security of personal information stored on portable devices. They ensure the use of new technologies meets security requirements for the protection of personal information, monitor adoption and implementation of such technologies and, where such monitoring identifies deficiencies or exposures, implement remedial action.
<b>Testing Security Safeguards (8.2.7)</b>	Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.	Tests of security safeguards for personal information are undocumented, incomplete and inconsistent.	Periodic tests of security safeguards are performed by the IT function; however, their scope varies.	Periodic and appropriate tests of security safeguards for personal information are performed in all significant areas of the business. Test work is completed by qualified personnel such as Certified Public Accountants, Chartered Accountants, Certified Information System Auditors, or internal auditors. Test results are documented and shared with appropriate stakeholders. Tests are performed at least annually.	Management monitors the testing process, ensures tests are conducted as required by policy, and takes remedial action for deficiencies identified.	Test results are analyzed, through a defined root-cause analysis, and remedial measures documented and implemented to improve the entity's security program.

GAPP - 73 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.



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.







Northwest  
Territories Internal Audit Bureau

MAR 07 2016

**CONFIDENTIAL**

MR. ERNIE CAMPBELL  
DEPUTY MINISTER  
ENVIRONMENT & NATURAL RESOURCES

**Forest Management Division EMBER System**

Enclosed is the above referenced Audit Report.

The Internal Audit Bureau will schedule a follow-up audit after October 2016.

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

T. Bob Shahi  
Director

Enclosure

- c. Mr. Mike Aumond, Chair, Audit Committee
- Mr. Bill Merklinger, Comptroller General, Finance
- Ms. Susan Craig, Director, Finance & Administration, ENR
- Mr. Frank Lepine, Director, Forest Management Division, ENR





Northwest  
Territories Internal Audit Bureau

## **Audit Report Operational Audit**

**Environment & Natural Resources  
Forest Management Division  
EMBER System**

**March 2016**

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



**CONFIDENTIAL**

March 7, 2016

File: 7820-21-ENR-151-114

MR. ERNIE CAMPBELL  
DEPUTY MINISTER  
ENVIRONMENT & NATURAL RESOURCES

**Audit Report: Forest Management Division EMBER System**  
**Audit Period: April 1, 2014 – November 30, 2015**

---

## **A. SCOPE AND OBJECTIVES**

The Audit Committee approved the Department of Environment and Natural Resources (ENR) management request for an audit of EMBER System used by Forest Management Division. The audit objectives were to:

- examine the governance framework to assess if the objectives of the EMBER system have been clearly defined and all the stakeholders know about them and how to achieve these objectives
- determine if preventive, detective and corrective controls were in place to ensure that relevant, complete, timely and accurate information was available to management
- assess that the established legislation, policy, contracts and procedures were following by stakeholder and monitored by management
- assess that assets (information, people, and equipment) were protected.

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



## **B. BACKGROUND**

The Forest Management Division used the EMBER System to track forest fire information. The audit contract was awarded to Grant Thornton by a Request of Proposal evaluation team composed of ENR 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 the EMBER System* made a number of observations and seven (7) recommendations.

No recommendations were required for the governance framework, oversight roles and responsibilities, or the EMBER reports used for decision making as these areas were well managed.

Four recommendations did not require any additional action as internal controls resided outside EMBER and management has either accepted the risk or the outstanding risk was low:

- 1) Absence of 'day of rest' tracking for individuals deployed on fire assignments
- 2) Absence of a documented process to reconcile EMBER and with Spatial Precipitation And Risk Calculation Imagery System
- 3) Incomplete data relating to fuel inventory within EMBER
- 4) Failure to carry out a Threat Risk Assessment (TRA) before implementation of EMBER.

Management developed action plans to address the risk identified in three areas:

- 1) Absence or inadequate documentation of system access controls within EMBER
- 2) Absence of a formal training program for staff using the EMBER system
- 3) Absence of a documented policy on system change management for EMBER.

The IAB will follow-up on the status of the management action plans for the three recommendations and inventory module after October 2016.



#### **D. ACKNOWLEDGEMENT**

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



T. Bob Shahi  
Director

# Government of the Northwest Territories

Department of Environment & Natural Resources

Forest Management Division



## Final Audit Report

### Audit of the EMBER System

---

February 2016

**TABLE OF CONTENTS**

<b>1.</b>	<b>EXECUTIVE SUMMARY</b> .....	<b>3</b>
<b>2</b>	<b>DETAILED AUDIT REPORT</b> .....	<b>8</b>
	<b>2.3.1 Governance</b> .....	<b>9</b>
	<b>2.3.2 Legislation, Policy, Contracts and Procedures</b> .....	<b>10</b>
	<b>2.3.3 Preventative, Detective, and Corrective Controls</b> .....	<b>12</b>
	<b>2.3.4 GNWT Assets</b> .....	<b>17</b>
	<b>APPENDIX A - AUDIT CRITERIA</b> .....	<b>19</b>
	<b>APPENDIX B – FINDINGS RATING SCALE</b> .....	<b>20</b>

## 1. EXECUTIVE SUMMARY

---

### 1.1 Background / Context

The Government of the Northwest Territories (GNWT) and the Department of Environment and Natural Resources (ENR) work to promote and support the sustainable use and development of natural resources to protect, conserve, and enhance the environment for the social and economic benefits of all residents.

One of the core objectives of ENR is to support the fire management activities within the Territory. In support of fire management activities, the Forest Management Division (FMD) within ENR uses the EMBER system to provide management with information to support decision making.

The EMBER system was implemented in the 2010 fire season. It has become the primary fire management software. Information contained within it includes smoke reports, initial fire assessments, fire responses, fire attributes, etc. It also contains administrative and financial information such as contracts, aircraft deployed, equipment used, resources assigned, fuel and materials used, and daily financial forecasts for each fire.

### 1.2 Audit Objectives and Scope

The objective of the audit was to assess whether information generated from the EMBER system is:

1. Timely and relevant for operating and senior management decision making; and
2. Reliable, complete and accurate.

The audit scope covered the period from April 1, 2014 to November 20, 2015. All transactions, events and operations related to the EMBER system during this time period were considered within the audit scope.

A site visit was conducted to the FMD office located in Fort Smith where process walkthroughs, audit testing and interviews were completed.

### 1.3 Summary of Observations and Recommendations

We identified a number of positive observations as well as opportunities for improvement, which are summarized below and further detailed in section 2.0.

The following positive observations were identified through the audit:

- Accountabilities related to the EMBER system have been defined, communicated and understood (i.e. the decision making authority for changes in EMBER resides with the Director, FMD within ENR)
- Reports from EMBER are being used for:
  - Management decision making purposes in the area of fire operations (i.e., daily response situation report, etc.); and
  - Sharing resource availability (i.e., resource allocation report and resource request report) with organizations such as, the Canadian Interagency Forest Fire Centre (CIFFC).<sup>1</sup>
- EMBER is used to forecast costs for fire operations to rationalize the supplementary budgets (also known as “special warrants”) through which additional funding from the Legislative Assembly is obtained.

---

<sup>1</sup> CIFFC - Canadian Interagency Forest Fire Centre Inc. is an organization that provides fire operations, management and information services to its Member Agencies that are comprised of all of the provinces, territories and the federal fire management agencies in Canada, as well as, the United States and other countries.

The table below aligns the areas audited with the two (2) main objectives. Opportunities for improvement and recommendations are linked to the audit objectives and classified and prioritized according to the impact on the organization (high, medium or low as defined in Appendix B – Findings Rating Scale). During our audit, we noted eight (8) key observations:

Audit Area	Objective 1	Objective 2	Key Observations	Impact Assessment	Report Section
1. Governance	✓		No observations noted	N/A	2.3.1
2. Legislation, Policy Contracts and Procedures	✓		<ul style="list-style-type: none"> <li>■ Day of rest guidelines</li> </ul>	Medium	2.3.2
3. Preventative, Detective, and Corrective Controls		✓	<ul style="list-style-type: none"> <li>■ System access controls</li> </ul>	Medium	2.3.3
			<ul style="list-style-type: none"> <li>■ Ember system training</li> </ul>	Low	
			<ul style="list-style-type: none"> <li>■ IT system change management</li> </ul>	Medium	
			<ul style="list-style-type: none"> <li>■ SPARC updates</li> </ul>	Low	
			<ul style="list-style-type: none"> <li>■ Fuel module data</li> </ul>	High	
4. GNWT Assets		✓	<ul style="list-style-type: none"> <li>■ Threat Risk Assessments</li> </ul>	Medium	2.3.4

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

### Key Observation 1: Day of Rest Guidelines

In accordance with the FMD’s Extra Duty Provisions, Work-Rest Guidelines, mandatory rest periods are stipulated for GNWT employees and contractors.

While EMBER tracks the deployment of crews to wildfires in the Territory, EMBER does not track the deployment of individual resources within fire crews.

During the audit, management indicated that there may be instances where individuals were deployed on fire assignments in which the maximum allowable consecutive working days was exceeded. Since the resource deployment reports did not capture individual deployment, the audit was unable to confirm these exceptions.

If individuals are being deployed on fire assignments after the maximum allowable consecutive working days, there is a risk of fatigue which could result in poor decision making in a high risk environment.

**Recommendation 1:** We recommend that the Director establish a process where an audit trail is maintained to demonstrate that resource deployment has not exceeded the maximum allowable days per the Work-Rest guidelines. Should exceptions be made, the process should be documented and clearly articulate who has the authorization to approve exceptions along with the reasons for the exception. In addition, we recommend that the Director assess the possibility of leveraging EMBER to assign a unique identifier per resource to facilitate the tracking and monitoring of resource deployment during the fire season.

### Key Observation 2: System Access Controls

During the audit, a list of EMBER users and their permissions was requested and obtained. Thirty-nine (39) users and one-hundred and seventy-eight (178) unique permissions (e.g.: change fire status) were identified by the audit team within this listing. Control gaps were found in the following areas:

- The listing of users did not contain the date the access was provided or the individual that requested and approved the access;
- Evidence of the user access requests and approvals were not maintained; and

- There was no evidence demonstrating that periodic reviews of the user access listing, or the reasonableness of the roles/permissions within the various EMBER modules was performed.

Without effective and documented access controls, there is a risk that the data contained within EMBER is not safeguarded and/or not secured from unauthorized access or unauthorized changes. Given the seasonal nature of the staff, there is also a risk that individuals no longer with the organization can continue to have access to the EMBER system.

**Recommendation 2:** We recommend that the Director, FMD:

- Establish a documented process to request, approve and remove access to EMBER which include specific roles within the various modules.
- Conduct periodic reviews of user access and their roles within the various modules be completed and documented by individuals approving access in EMBER.

### **Key Observation 3: EMBER System Training**

The audit noted that an EMBER training program has been drafted, but not yet finalized. The training program identifies what training is required and the frequency with which training should occur. A training matrix has been developed which identifies what training is required for the various roles within EMBER. Given that management relies on the EMBER system to make key decisions during the fire season, not providing comprehensive, formalized and consistent training could result in poor quality information being entered into the EMBER system.

**Recommendation 3:** We recommend that the Director, FMD finalize the training program and establish a training plan identifying resources and materials to support staff in understanding procedures for entering complete, accurate, timely and relevant information into EMBER.

### **Key Observation 4: IT System Change Management**

In May 2015, updates were made to the EMBER system to enhance its reporting functionalities and to introduce additional features. There was a lack of documentation around how business needs were identified, prioritized, approved, and implemented.

Management indicated that a GNWT Policy on change management related to systems and technology was currently not in place. As a result, system change management process and analysis was not formalized or documented in accordance with best practices (e.g., documenting a business needs analysis, changes are implemented in a testing environment before impacting the production environment, etc.).

There is a risk that system changes were not appropriately prioritized and tested which could result in unplanned system outages or unavailability of data impacting the timeliness and relevance of reports for decision making.

**Recommendation 4:** We recommend that the Informatics Shared Services group adopt COBIT to develop a policy for systems change, including changes to EMBER. We recommend that for the EMBER system, the identification, prioritization and approval of changes, as well as, implementation (testing) performed be documented.

### **Key Observation 5: SPARC Updates**

On a daily basis, the SPARC report is compared / reconciled with the EMBER statistics. If discrepancies are found (i.e. latitude and longitude, size of the fire, or the attributes of the fire including rate of spread, wind, smoke characteristics, etc.), the fire clerk update that EMBER records.

For the audit sample testing, it was noted that for the seventeen (17) files tested, all the data fields within EMBER were completed and there were edits made to correct discrepancies found. Although the edits to the individual fires within the EMBER system may have been due to updates detected through SPARC, there was no documented evidence demonstrating that a reconciliation between SPARC and EMBER occurred. Therefore, audit was unable to determine the operating effectiveness of this control.

Without evidence to demonstrate that corrections or updates are made to the EMBER system fire records based on information detected from the SPARC system, there is a risk that incomplete, inaccurate, irrelevant and untimely information resides in EMBER that cannot be relied upon.

**Recommendation 5:** We recommend that the Director, FMD document the reconciliation process between EMBER and SPARC, and that the process document be approved by ENR.

### **Key Observation 6: Fuel Module Data**

During the audit, the following discrepancies related to the fuel module were observed:

- Fuel information was not updated when transferred in/out, resulting in negative inventory values at three (3) fuel caches; and
- For 151 transactions, the EMBER system indicated that jet fuel was consumed before the production date.

Data within the fuel module is unreliable due to delays in entering the information. Users of the system indicated that procedures to update the fuel module are informally communicated, enforced and monitored. Unreliable information within the fuel module could result in inefficient and ineffective transfers of fuel between locations, and discarding or misuse of fuel which has past the expiry date.

**Recommendation 6:** We recommend that the Director, FMD:

- Communicate and monitor compliance to procedures within the fuel module to facilitate the entry of timely, reliable information in EMBER; and
- Consider implementing preventative controls within the fuel module such that, negative amounts of fuel cannot be entered or exist on hand.

### **Key Observation 7: Threat Risk Assessment (TRA)**

The GNWT Policy on Electronic Information Security requires that a Threat Risk Assessment (TRA) be completed for all information assets, including EMBER.

At the time of the audit, a TRA had not been completed. Without a TRA, there is a risk that weaknesses related to IT security controls surrounding the confidentiality, integrity, availability, security and privacy of the data within EMBER are not identified and addressed in a timely manner. Given the criticality of the business operations during the fire season, should such vulnerabilities be left unattended, there are increased risk exposures that could compromise the accuracy, timeliness, availability, reliability and completeness of the information within EMBER.

**Recommendation 7:** We recommend that in compliance with GNWT's Information Technology Electronic Information Security Policy, a Threat Risk Assessment (TRA) be completed for EMBER.

## **1.4 Conclusion**

### Objective 1:

As a mission critical system for business operations, the EMBER system produces timely and relevant reporting for senior management to enable informed decision making. Key reports in which management relies upon

included, the Daily Response Situation Report, the Weekly Forest Fire Management Report and the CIFFC Worksheet Report. Additionally, IT governance was found to be appropriate for the criticality and complexity of the EMBER system.

Objective 2:

Although EMBER reports were deemed to be timely and relevant, the audit found that certain components of the reports, specifically around the fuel model could not be considered reliable, complete or accurate. Control design and documentation improvements in the areas of system access control, training, data reconciliations and system change management should be strengthened to further enhance the reliability of data within the EMBER system.



## 2 DETAILED AUDIT REPORT

---

This section presents detailed findings from the EMBER System 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:

The Government of the Northwest Territories (GNWT) and the Department of Environment and Natural Resources (ENR) work to promote and support the sustainable use and development of natural resources to protect, conserve, and enhance the environment for the social and economic benefits of all residents.

One of the core objectives of ENR is to support the fire management activities within the Territory. In support of fire management activities, the Forest Management Division (FMD) within ENR uses the EMBER system to provide management with information to support decision making.

The EMBER system was implemented in the 2010 fire season. It has become the primary fire management software. Information contained within it includes smoke reports, initial fire assessments, fire responses, fire attributes, etc. It also contains administrative and financial information such as contracts, aircraft deployed, equipment used, resources assigned, fuel and materials used, and daily financial forecasts for each fire.

There are four (4) main modules in the EMBER system: the operations and maintenance, aircraft, fuel, and the reporting module. EMBER is not a web-based system, it is in fact, a desktop based application and does not interface with the financial system SAM or other systems.

There are several reports generated from EMBER that are being used for:

- Management decision making purposes in the area of fire operations (i.e., daily response situation report, etc.); and
- Resource planning including sharing of resources (i.e., resource allocation report and resource request report) with organizations such as, the Canadian Interagency Forest Fire Centre (CIFFC).

Although EMBER is the mission critical system for fire operations, management and financial forecasting for suppression activities, it has no mapping interface or spatial abilities. Therefore, supporting systems, such as, SPARC (web based) which was developed in-house within FMD is used. As such, there is no duplication of effort between EMBER and SPARC since SPARC extracts data directly from EMBER.

SPARC creates fire statistics, predictive analytics and data modelling leveraging information gathered through satellite imagery and building this onto information (such as location, area and fire characteristics) extracted from EMBER in real time. Potential errors in EMBER are detected using and comparing data models and reports in SPARC.

### 2.2 Focus of the Internal Audit:

The objective of the audit was to assess whether information generated from the EMBER system is:

- Timely and relevant for operating and senior management decision making; and
- Reliable, complete and accurate.

The audit scope covered the period from April 1, 2014 to November 20, 2015. All transactions, events and operations related to the EMBER system during this time period were considered within the audit scope.

A site visit was conducted to the FMD office located in Fort Smith where process walkthroughs, audit testing and interviews were completed.

### **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 examined the extent to which the governance for the EMBER system is established, communicated and being adhered to. In particular, the audit assessed:

- Oversight, roles and responsibilities;
- EMBER reports and management decision making; and

#### **Oversight, Roles and Responsibilities:**

Through interviews, it was indicated that ENR are the owners of EMBER. The oversight for the EMBER system is held with the Director, FMD within ENR who provides the final approval for changes to the EMBER system.

Decision making for fire operations and management is established through roles and responsibilities assigned to the fire clerks, Regional Duty Officers (RDO), Territorial Duty Officers (TDO), Manager and the Director of the FMD within the EMBER System. Roles and responsibilities have been documented within approved job descriptions for individuals along with the tasks expected of them within EMBER. Although not formally documented, through interviews, it was noted that key individuals understood their roles and responsibilities within EMBER.

#### **EMBER Reports and Management Decision Making:**

There are several “standard” reports (over 25) which can be generated from the EMBER system. In addition, customized reports can also be generated within the various EMBER modules based on the information contained within EMBER. Management indicated that these key reports are used and relied upon for management decisions throughout the fire season as well as for budgeting and forecasting purposes.

A sample of the key EMBER reports, a brief description of what information is contained within them and how they are being used by management is provided below.

#### **Daily Response Situation Report (Standard EMBER Report):**

The Daily Response Situation Report is generated manually on a daily basis within Fort Smith. It contains information on the fire number, the location and size per fire, the date and time the fire was last monitored, the response taken for the fire, the fire’s current status, as well as, any other relevant comments regarding the fires.

Management within Fort Smith use this report to monitor the reasonability of the responses and the status of the fires. Management manually compares this to the previous day’s report for any significant changes. The audit obtained a sample of ten (10) days during the 2015 fire season and noted that the daily response situation report was printed and on file (stored within Fort Smith). In addition, evidence of manual review by management was noted. No exceptions were noted.

Weekly Forest Fire Management Report (Customized EMBER Report):

This report is manually generated by management within Fort Smith. It is a customized report that primarily derives information from various reports in EMBER. It includes the estimated expenditures for fire suppression activities by cost category, such as staff, aircraft contracts, commitments for various accounts payable vendors, assistance claims and recoveries from other organizations when sharing resources.

This report is used on a weekly basis to monitor the expenditures incurred for the aircraft contracts. It is also used to closely monitor the commitments and related expenses incurred for the local vendors. Given that there is often a delay in the vendor invoices being entered into the financial system, having more timely financial information within EMBER is useful for management to monitor financial spend through this report. Standard Reports from EMBER such as the Forest Fire Activity to Date Report, the YTD Amount by Program Report and the YTD Amounts by Summary Program was used to support the weekly Forest Fire Management Report. The audit obtained a sample of five (5) weekly reports during the fire season and noted that they were completed in full and the supporting EMBER reports were documented and saved in file. No exceptions were noted.

CIFFC Worksheet (Standard EMBER Report):

During the fire season, the CIFFC Worksheet report is generated daily by management within Fort Smith. This report shows all the fire operations and management related activities for each region within the GNWT over the past 24 hours. The report contains the number of fires per region that are currently burning along with the total land area. It also has the total number of fires per response type and the total area of land associated with these fires. This report is a snapshot of the fires and the severity of the fires for the GNWT at any given time. It is used to create the CIFFC worksheet that is submitted online. This is a mandatory exercise that has to be completed by ENR as the GNWT is a partner in the CIFFC program.

The audit obtained a sample of ten (10) days during the 2015 fire season and noted that the CIFFC worksheet was completed in a timely manner and reviewed by the Regional Duty Officer. The supporting EMBER Reports for each of the CIFFC worksheets were also reviewed to evaluate the accuracy of the worksheets completed. No exceptions were noted.

**2.3.2 Legislation, Policy, Contracts and Procedures**

There are several legislation, policies and procedures in place with respect to contracting, fire operations, management, as well as, financial forecasting and budgeting as it relates to the EMBER system. The audit focused on the following:

- Forest Fire Management Policy;
- Business Incentive Policy;
- Days of Rest Guideline; and
- Financial Administration Manual.

**Forest Fire Management Policy:**

The Forest Fire Management Policy is the overarching GNWT policy that identifies the role and responsibilities of the GNWT with respect to forest fire management. The policy requires that fire management should strive to attain forest management and other land use objectives in a manner that considers environmental, social, and economic criteria. The Forest Fire Management Policy indicates that decisions and prioritizing fire suppression activities should be based on the Value at Risk (VAR).

The VAR for each fire is based on a hierarchical assessment of Human Life; Property; Natural Resource values<sup>2</sup> and Cultural Resource values. As such, VAR relates to human life, natural or cultural resources that have measurable or intrinsic worth and that could or may be destroyed or altered by a fire in any given area. This means that in developing a strategy to manage and prioritize fires, the first consideration in the allocation of fire management resources is given for the protection of human life. All other considerations take into account the relative value of the resources that may be destroyed or otherwise altered by the forest fire.

During the audit, a sample of seventeen (17) fires were tested. For each of these fires the VAR was included and considered during the decision making process, no exceptions noted.

#### **Business Incentive Policy:**

On an annual basis, Standing Offer Agreements (SOA) are established with fixed wing and rotary aircraft providers for fire management services. As a procurement vehicle, the SOAs should be established in accordance with the GNWT Business Incentive Policy (BIP). The BIP provides an incentive to Northwest Territories-based businesses in a manner that recognizes the higher cost of operating businesses and manufacturing products in the Northwest Territories.

During the audit, the SOAs were tested to assess if they were created in accordance with the BIP. The audit also tested if call-ups against the SOAs were in accordance with the terms and conditions of the SOAs.

Our audit tests indicated that for two (2) of the three (3) SOAs, the supplier was registered in accordance with the BIP. Given that one (1) of the samples tested included a supplier from Alberta, the BIP policy was not relevant to that SOA.

Our audit tests also indicated that for all of the three (3) samples selected, call ups against SOAs were performed by the Supervisor, Aviation Services based on resource availability and proximity to fires. The call-ups were in accordance with the terms of the SOA (e.g.: the rate per hour was accurate). All required information on contractors, including aircraft and pilot information was complete and accurate. No exceptions were noted.

#### **Extra Duty Provisions, Work-Rest Guidelines:**

In accordance with the FMD Extra Duty Provisions, Work-Rest Guidelines, mandatory rest periods are stipulated for GNWT employees and contractors.

While EMBER tracks the deployment of crews to wildfires in the Territory, EMBER does not track the deployment of individual resources within fire crews. Therefore, EMBER does not provide FMD management with complete information in order to ensure that the guideline is being followed.

To mitigate the risks of non-compliance with the guideline, management indicated that informal tools, such as “whiteboard schedules”, are used by the regions during the fire season. During the audit, management indicated that there may be instances where individuals are being deployed on fire assignments exceeding the maximum allowable consecutive working days. However, since the resource deployment reports did not capture individual deployment, the audit was unable to confirm these exceptions.

If individuals are being deployed on fire assignments after the maximum allowable consecutive working days, there is a risk of fatigue which could result in poor decision making in a high risk environment.

#### **Recommendation #1:**

We recommend that the Director establish a process where an audit trail is maintained to demonstrate that resource deployment has not exceeded the maximum allowable days per the Work-Rest guidelines. Should

---

<sup>2</sup> Natural Resource values includes primary wildlife harvesting areas, commercial timber areas, endangered species areas

exceptions be made, the process should be document and clearly articulate who has the authorization to approve exceptions along with the reasons for the exception. In addition, we recommend that the Director assess the possibility of leveraging EMBER to assign a unique identifier per resource to facilitate the tracking and monitoring of resource deployment during the fire season.

**Management Response to Recommendation #1:**

Controls with regards to the rest days are exercised outside the EMBER system using PeopleSoft which is the system of record for payroll and human resources within the GNWT. Supervisors and Regional Duty Officers (RDOs) are responsible for managing and monitoring the rest periods for staff under their control. Reports from PeopleSoft shall be used to check for the exceptions, and serve as audit trail. No additional modifications or changes will be made to the EMBER system as this process is managed using PeopleSoft information.

**Financial Administration Manual:**

In accordance with sections 28 and 29 of the *Financial Administration Act (FAA)*, the GNWT prepares annual budgets, called Main Estimates, for Legislative Assembly approval. ENR is thereby allocated a budget (main estimates) for fire suppression. A Special Warrant is a mechanism that GNWT departments can use to request an immediate increase to their approved annual budgets for expenditures that are urgently required. The GNWT is required to adequately substantiate the urgency of the request to the Financial Management Board within the GNWT. The final approval of a Special Warrant resides with the Commissioner of the Northwest Territories.

During our audit, we reviewed the requests for supplementary budgets (special warrants) to the main estimates for both the 2014 and the 2015 fire seasons. We noted that the requests were created based on the projected fire suppression costs supported by EMBER reports. Since EMBER is the primary financial forecasting tool for fire suppression activities, it is heavily relied upon to develop the financial forecasts for the fire season. Detailed analysis, predictive models and cost rationalization for each cost category is prepared and documented. The special warrants were appropriately approved for the amount of funding requested. No exceptions were noted.

Fire suppression is a significant expenditure for the GNWT, the total forecast for the 2015 fire season was \$31.8 million in EMBER with the actual costs amounting to \$30.8 million. Given that each fire can cause considerable harm, the department's priority is protecting human life, property, natural resources, as well as, cultural resources.

A variance analysis between forecasted amounts for fire suppression and actual costs for fire suppression was completed and documented. A high level variance analysis between the actual costs to the forecasted fire suppression costs was performed following the fire season in 2014.

**2.3.3 Preventative, Detective, and Corrective Controls**

The Institute of Internal Auditors defines *Control* as any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.<sup>3</sup>

---

<sup>3</sup> Institute of Internal Auditors Standards, S. 2130

### **Preventative Controls:**

Preventative controls are controls in place to help prevent specific actions from occurring. During the audit, three (3) primary preventative controls were examined, including:

- Access controls (request, approval, changes, termination of access and periodic reviews);
- Training for the EMBER system; and
- IT System Change Management.

### **Access Controls:**

EMBER is installed on local GNWT desktops. In order to access the GNWT desktops, the users need to have an approved/authorized user name and password, upon which they can access the system. EMBER is available to individuals who reside both within the regional offices, as well as, the head office in Fort Smith. It is provided to employees within ENR, as well as, seasonal staff who are employed during the fire season. The process for requesting, changing access or terminating access for an EMBER account is not formally established or documented. A request is received from a Regional Duty Officer by email or phone to create a user account.

During the audit, a list of EMBER users and their permissions was requested and obtained. Thirty-nine (39) users and one-hundred and seventy-eight (178) unique permissions (e.g.: change fire status) were identified by the audit team within this listing. Control gaps were found in the following areas:

- The listing of users did not contain the date the access was provided or the individual that requested and approved the access;
- Evidence of the user access requests and approvals were not maintained; and
- There was no evidence demonstrating that periodic reviews of the user access listing, or the reasonableness of the roles/permissions within the various EMBER modules is performed.

Without effective and documented access controls, there is a risk that the data contained within EMBER is not safeguarded and/or not secured from unauthorized access or unauthorized changes. Given the seasonal nature of the staff, there is also a risk that individuals no longer with the organization can continue to have access to the EMBER system.

### **Recommendation # 2:**

We recommend that the Director, FMD:

- Establish a documented process to request, approve and remove access to EMBER which include specific roles within the various modules.
- Conduct periodic reviews of user access and their roles within the various modules be completed and documented by individuals approving access in EMBER.

### **Management Response to Recommendation #2:**

The FMD Director, with assistance from Informatics, will create a protocol for approving access and removal of users to EMBER prior to the 2016 fire season.

### **Training for the EMBER system:**

Training is considered a preventative control for the EMBER system as the quality (completeness, accuracy, timeliness and reliability) of the EMBER reports are dependent on the quality of the information entered into

the system. Training to ensure that staff understand the required information, including the level of detail to be entered in the system would improve the overall quality of the information.

Within FMD, the group of EMBER users includes both permanent full time employees as well as seasonal staff hired during the fire season and located throughout the Territory. Amongst the seasonal employees are Fire Clerks, who are responsible for entering fire information in EMBER during fire season. As the information entered by Fire Clerks is used by management to make decisions with respect to fire suppression and management activities, it is critical that EMBER users, including seasonal staff, receive sufficient training on the EMBER system and related policies including the requirements of the Forest Fire Management Policy.

The audit noted that an EMBER training program has been drafted, but not yet finalized. The training program identifies what training is required and the frequency with which training should occur. A training matrix has been developed which identifies what training is required for the various roles within EMBER. Given that management relies on the EMBER system to make key decisions during the fire season, not providing comprehensive, formalized and consistent training could result in poor quality information being entered into the EMBER system.

### **Recommendation #3:**

We recommend that the Director, FMD finalize the training program and establish a training plan identifying resources and materials to support staff in understanding procedures for entering complete, accurate, timely and relevant information into EMBER.

### **Management Response to Recommendation #3:**

The FMD Director will formalize the EMBER training plan to ensure a comprehensive understanding of information requirements within EMBER for all authorized uses prior to the 2016 fire season.

### **Information Technology (IT) System Change Management (Change Control):**

Control Objectives for Information and Related Technology (COBIT) is a leading practice IT framework that helps define key governance and technical controls within an organizations IT environment. COBIT 4.1 - processes associated with IT change management provides the following guidance around IT system change management:

*“All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following the implementation. This process assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.”<sup>4</sup>*

For IT system changes, standardized methods and procedures are used for efficient and prompt handling of IT changes, in order to minimize the number and impact of any related incidents upon service. This entails several steps, some of which include established criteria for evaluating identified changes (user needs) and prioritizing the system changes, approving the changes, testing the changes in the development environment prior to release in the production environment, scheduling and implementing the release of changes and implementing them. It would be expected that these steps would be documented to demonstrate the procedures were completed to maintain an audit trail.

---

<sup>4</sup> IT Governance Institute, COBIT 4.1, USA, 2007

In May 2015, updates were made to the EMBER system to enhance its reporting functionalities and to introduce additional features. There was a lack of documentation around how business needs were identified, prioritized, approved, and implemented.

Management indicated that there is currently no GNWT Policy on change management related to systems and technology. As a result, changes to EMBER tend to occur in an ad hoc manner as opposed to a formalized process developed in accordance with best practices (e.g.: changes are implemented in a testing environment before impacting live information).

There is a risk that system changes are not appropriately prioritized and tested which could result in unplanned system outages or unavailability of data impacting the timeliness and relevance of reports for decision making.

**Recommendation #4:**

We recommend that the Informatics Shared Services group adopt COBIT to develop a policy for systems change, including changes to EMBER. We recommend that for the EMBER system, the identification, prioritization and approval of changes, as well as, implementation (testing) performed be documented.

**Management Response to Recommendation #4:**

Effective immediately, all changes made to EMBER system will be authorized by the FMD Director and Informatics will identify, prioritize, document and test any changes made to EMBER before implementation using industry standards.

**Detective and Corrective Controls:**

Detective controls are established to detect the occurrence of specific events or errors after they occur. Examples of detective controls may include, but are not limited to:

- Review of reports; and
- Review of records after they are entered into the system.

Information is manually entered into the EMBER system by the fire clerks when creating a fire record. This includes the smoke report, the initial fire assessment, fire response, related updates, and the daily financial forecasts per fire. There were 241 fires logged in the EMBER system for the 2015 fire season.

During the course of the audit, management indicated that the Spatial Precipitation and Risk Calculation (SPARC) system runs fire statistics, predictive modelling and fire analytics based on live data from satellite imagery and is used as a detective control mechanism to identify any “missed” entries in EMBER.

On a daily basis, the SPARC report is compared / reconciled with the EMBER statistics. If discrepancies are found (i.e. latitude and longitude, size of the fire, or the attributes of the fire including rate of spread, wind, smoke characteristics, etc.), the fire clerk update that EMBER records.

For the audit sample testing, it was noted that for the seventeen (17) files tested, all the data fields within EMBER were completed and there were edits made to correct discrepancies found. Although the edits to the individual fires within the EMBER system may have been due to updates detected through SPARC, there was no documented evidence demonstrating that a reconciliation between SPARC and EMBER occurred. Therefore, audit was unable to determine the operating effectiveness of this control.

Without evidence to demonstrate that corrections or updates are made to the EMBER system fire records based on information detected from the SPARC system, there is a risk that incomplete, inaccurate, irrelevant and untimely information resides in EMBER that cannot be relied upon.



**Recommendation #5:**

We recommend that the Director, FMD document the reconciliation process between EMBER and SPARC, and that the process document be approved by ENR.

**Management Response to Recommendation #5:**

Management is aware of the observation and accepts the risk. Other controls outside the EMBER system are used to ensure that data input in the system from SPARC is reasonably accurate and reliable.

Corrective controls are controls that restore systems or processes to the state prior to the occurrence of the detected event. During the audit, it was observed that manual corrective controls are applied to information within EMBER on an ad hoc basis. Examples of the types of controls applied include, but are not limited to:

- The correction of inventory levels in fuel caches to remove negative inventory balances;
- The correction of areas burned based on satellite imagery; and
- The correction of fire information deemed to be incorrect.

The corrective controls occur outside of fire season due to the operational focus of staff during fire season, and therefore were not impactful for management decision made during fire season.

During the audit, issues related to bandwidth and low connectivity when using EMBER, especially in remote regions within the GNWT were identified by several key officers. During the fire season, these issues were identified by individuals and communicated to the IT help desk (INFOMATICS). The audit tested the IT help tickets logged from May 1 to August 31, 2015 (covering the 2015 fire season) which showed a total of 45 issues raised and resolved, of which 31 issues were related to synchronization problems with the EMBER system. These issues were resolved in a reasonable manner and did not impact the completeness or timeliness of the information within EMBER.

**Fuel Module Data**

Within the EMBER system, fuel information is logged, updated, tracked and monitored. This information is critical since its completeness, accuracy, timeliness and relevance determines the quality and reliability of the reports that are generated for decision making for fire operations, management and financial forecasts.

Fuel inventories including purchasing, consumption and storage information is required to be documented in the Fuel Module within EMBER. Management relies on the accuracy of this information to make critical decisions such as the deployment of contracted aircraft and fire crews to fight wildfires, purchasing and transfer information. In addition, reliable fuel information helps ensure that fuel does not exceed one year past its production date, which is considered to be expired based on industry standards.

During the audit, the following discrepancies related to the fuel module were observed:

- Fuel information was not updated when transferred in/out, resulting in negative inventory values at three (3) fuel caches; and
- For 151 transactions, the EMBER system indicated that jet fuel was consumed before the production date.

Data within the fuel module is unreliable due to delays in entering the information. Users of the system indicated that procedures to update the fuel module are informally communicated, enforced and monitored. Unreliable information within the fuel module could result in inefficient and ineffective transfers of fuel between locations, and discarding or misuse of fuel.

**Recommendation #6:**

We recommend that the Director, FMD:

- Communicate and monitor compliance to procedures within the fuel module to facilitate the entry of timely, reliable information in EMBER; and
- Consider implementing preventative controls within the fuel module such that, negative amounts of fuel cannot be entered or exist on hand.

**Management Response to Recommendation #6:**

Management acknowledges the recommendation. No modifications to EMBER will be made at this time. At the start of each fire season, FMD Director will provide briefing to all users regarding the data entry of inventory in timely manner.

FMD Director has a number of internal control measures outside EMBER to ensure that expired fuel is not used;

- All fuel that may be expired is recertified.
- Air crafts are provided with staff and fuel technicians independent of GNWT staff or EMBER for independent testing of fuel.

**2.3.4 GNWT Assets**

The GNWT Policy on Electronic Information Security applies to all electronic information assets and the underlying technologies used in the creation, maintenance, processing, storing, transmission, or disposition of information within or by the GNWT. The policy recognizes that the increased use of information technologies to serve the public and to record its business requires that electronic information assets collected or made available electronically must be maintained in an environment that protects the confidentiality, availability, and integrity of the information over time and through technology change. The policy assigns accountability for all elements of information security, including:

- Conducting threat and risk assessments and data classification for all information assets
- The implementation of appropriate security measures to protect the integrity, availability and confidentiality of information contained within the asset consistent with those published in the GNWT Standard of Best Practice for Information Security Management
- Formalizing security measures in a written document

The GNWT Policy on Electronic Information Security requires that a Threat Risk Assessment (TRA) be completed for systems such as the EMBER system.

At the time of the audit, a TRA had not been completed. Without a TRA, there is a risk that weaknesses related to IT security controls surrounding the confidentiality, integrity, availability and security of the data within EMBER are not identified and addressed in a timely manner. Given the criticality of the business operations during the fire season, should such vulnerabilities be left unattended, there are increased risk exposures that could compromise the accuracy, timeliness, availability, reliability and completeness of the information within EMBER.

**Recommendation #7:**

We recommend that in compliance with GNWT's Information Technology Electronic Information Security Policy, a Threat Risk Assessment (TRA) be completed for EMBER.

**Management Response to Recommendation # 7:**

Management acknowledges the recommendation. This audit was helpful in identifying a number of issues that would normally be identified during a TRA. Emphasis will be put on rectifying the areas of weaknesses already identified and a TRA will be done at such a time when there is a major modification within the system. The risk is well managed.

## 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 Focus	Audit Criteria
<b>1. Governance</b>	Examine the extent to which a governance structure has been developed, is clear, and supports effective decision making with respect to fire management and suppression activities.	<p><b>1.1</b> The governance structure, decision making authority within the oversight mechanisms, as well as, the roles and responsibilities related to the EMBER system have been established and are being adhered to.</p> <p><b>1.2</b> The objectives of the EMBER system have been clearly defined and all the stakeholders (e.g.: contractors management, staff, etc.) are aware of the objectives and how to achieve them.</p>
<b>2. Legislation, Policy, Contracts, and Procedures</b>	Examine the extent to which appropriate legislation, policies, contracts and procedures are followed.	<p><b>2.1</b> Appropriate policies, procedures, legislation, and contracts have been established, approved and communicated. Mechanisms are established to assess compliance to these with corrective actions as required.</p> <p><b>2.2</b> Controls have been established in accordance with GNWT policies, procedures, legislation, and contract requirements and are operating effectively.</p>
<b>3. Preventative, Detective, and Corrective Controls</b>	Examine the extent to which management receives timely, complete, accurate and reliable reports from the EMBER system to enable informed decision making.	<p><b>3.1</b> Controls are in place to ensure that relevant, complete, timely and accurate information is entered into EMBER, available to management (reports) and used for decision making, as well as, monitoring activities.</p> <p><b>3.2</b> Controls related to EMBER access, segregation of duties, in EMBER and IT change management in EMBER are in place and are operating effectively.</p>
<b>4. GNWT Assets</b>	Examine the extent to which GNWT assets is safeguarded within the EMBER system.	<b>4.1</b> Controls have been established in accordance with GNWT policies on the security of information for the EMBER system.

## APPENDIX B – FINDINGS RATING SCALE

Our findings are classified and prioritized according to impact on the organization using the following definitions:

Findings Legend	
Impact Rating	Explanation
<b>High</b>	<ul style="list-style-type: none"> <li>■ Must be addressed in short term (90- 120 days/ 3-4 months).</li> <li>■ Findings could result in significant risk exposure (e.g. reputational, financial) or impact the ability of achieving objectives.</li> <li>■ Findings could impact the completeness, accuracy, relevancy and/or timeliness of information entered into EMBER and the reliability of resultant reports.</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>■ Should be addressed in the medium term (180- 270 days/ 6-9 months)</li> <li>■ Findings could result in risk exposure or financial impact and cause financial mismanagement.</li> </ul>
<b>Low</b>	<ul style="list-style-type: none"> <li>■ Findings identify areas for improvement to optimize fire operations and management.</li> <li>■ Opportunities for business process enhancements to improve value for money.</li> </ul>



**CONFIDENTIAL**

June 7, 2019

File: 7820-20-GNWT-151-135

DR. JOE DRAGON  
DEPUTY MINISTER  
ENVIRONMENT & NATURAL RESOURCES

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

---

**A. SCOPE AND OBJECTIVES**

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

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

**B. BACKGROUND**

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

- Regulatory Revenues such as Environment fund, Hunting and Fishing licenses, fees for water and soil analysis
- Service and Miscellaneous revenue.

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

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

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

## C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The audit report, *“Department of Environment & Natural Resources, Revenue Process Audit Report,”* made several observations and recommendations specific to ENR (**Schedule I refers**).

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

- Compliance with IB 620.01 (collection of accounts receivable)
- Partial compliance with IB 610.01 (rationale for the fee charged).

The contractor was unable to find sufficient documentary evidence to assess compliance:

- FAM 605 (recording revenue)
- FAM 610 (establishment of fees)
- FAM 620 (collection of receivables).

In examining the internal control capacity for the six revenue processes, the contractor assessed that there were gaps in the five areas.

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

ENR Revenue Process Area	Internal Control Capacity Level	
	Current	Required
Role definition and responsibility	3	3
Rate setting and review	1	3
Budget setting	2	3
Invoicing	2	3
Accounts receivable review / collection	2	3
Monitoring	2	3

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

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

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

**D. ACKNOWLEDGEMENT**

We want to thank the ENR staff for their assistance and co-operation throughout the audit.

T. Bob Shahi  
 Director, Internal Audit Bureau  
 Finance



## **SCHEDULE I**

**DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES**

**REVENUE PROCESS AUDIT REPORT**

## DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

### SCOPE AND OBJECTIVES

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

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

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

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

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

### DEPARTMENTAL BACKGROUND

The Department of Environment and Natural Resources (ENR) meets its responsibilities through the following functions:

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

General revenues generated by ENR consist of the following:

- Regulatory Revenue - Environment fund revenues; Fees for water and soil analysis, Hunting and fishing licenses, Timber permits and licenses, and Spill recovery;
- Services and Miscellaneous – Service recoveries.

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

- Environment fund revenues are the responsibility of Environment Fund Officers.
- Fees for water and soil analysis are the responsibility of Taiga Labs Office Coordinator with support from the Manager, Corporate Services and Corporate Services Officer.

- Hunting and Fishing Licenses are the responsibility of the Regional Senior Corporate Services Officer.
- Timber permits and licenses are the responsibility of the Compliance Forester, Forest Management Division.
- Spill recovery is the responsibility of the Environmental Protection Manager.
- Service recoveries are the responsibility of environment fund officers.

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

## METHODOLOGY

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

## OVERVIEW

### Compliance with FAA and FAM

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

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

Based on the audit work performed, as well as the inability of the ENR department to provide the evidence necessary to conclude on internal control effectiveness, Crowe has concluded that additional work is required by ENR to design and implement internal controls to sustain an audit opinion of "Compliant". This will include the necessary documentation required to support that key controls are operating effectively. Support for this assessment is provided in the following table:

Section Policy	Compliance Assessment	Reason for Non-Compliance
<b>605 – Recording Revenue</b>		
Revenue earned for work performed, goods supplied, services rendered, or amounts entitled in the fiscal year must be recorded in accordance with approved systems and procedures in a timely manner.	<b>Unverifiable</b>	Unable to verify if revenue earned is recorded in accordance with approved systems and procedures because not all approved systems and procedures are documented.

Section Policy	Compliance Assessment	Reason for Non-Compliance
<b>610 – Establishment of Fees</b>		
<p>Where economically and administratively feasible, GNWT Departments and Public Agencies shall charge fees for licenses, permits and services rendered to the public. The authorized rates for any fee shall bear a reasonable relationship to the cost of administering the license or service or be authorized at a rate lower than full cost recovery, where appropriate.</p>	<b>Unverifiable</b>	<p>Rates for non-regulated items are not reviewed on a set basis.</p> <p>Regulated rates are reviewed every five year as per FMB direction.</p> <p>The rationale for rate changes or unchanged rates at the five year review are not documented as such it is not verifiable whether the rates address current costs of the related services or license.</p>
<p><b>IB610.01 Rationale for Fees Charged</b></p> <p>GNWT Departments and Public Agencies are to ensure that fees are collected, safeguarded, and accounted for. A rationale for each fee charged must be kept available for audit purposes.</p> <p>The rationale in support of each fee charged must include:</p> <ul style="list-style-type: none"> <li>- pricing details;</li> <li>- the price/rate basis, including direct, indirect, and accounting and system costs; and,</li> <li>- the time period for cyclical fee reviews.</li> </ul> <p>In the case of a regulatory service, a fee or charge fixed on a total cost recovery basis may not be warranted. The fee for such a service may be collected from the ultimate user or from an intermediary who considers the expense a cost of doing business.</p>	<b>Partially Compliant</b>	<p>Pricing details and price/rate basis are included for all revenue streams. Some revenue streams have set period review cycles.</p> <p>Some revenue streams do not have documented periodic fee reviews. In some cases this is due to a legislated fee structure; for these there should be a documented cyclical review period for the legislation in regards to fee aspects.</p>
<b>620 – Collection of Receivables</b>		
<p>GNWT Departments and Public Agencies are responsible to collect all accounts receivable promptly, efficiently, and in a thoroughly accountable manner, unless otherwise directed by the Comptroller General or their delegate.</p>	<b>Unverifiable</b>	<p>Please refer to Observation 8 – there are some long outstanding AR balances coded to "On Account" for ENR that have not been cleared, therefore it is not possible to verify that all accounts receivable were received in a timely and accountable manner.</p>
<p><b>IB 620.01 Collection of Accounts Receivable</b></p> <p>Except as described below, an invoice must be prepared, recorded, and delivered to the debtor as soon as a receivable is created and the debtor must be given 30</p>	<b>Compliant</b>	<p>Revenues on account are invoiced and the debtor is provided 30 days from the date of invoice to make</p>

Section Policy	Compliance Assessment	Reason for Non-Compliance
<p>calendar days from the date of the invoice to return payment to the GNWT or Public Agency.</p> <p>If payment is not received within 30 days of the date of the invoice, the responsible department or Public Agency shall attempt to collect by notifying the debtor in writing that payment is overdue and payable immediately. At this point, the debt has become an overdue receivable.</p> <p>If payment is not received during the next 30 days (i.e., within 60 days of the date of the invoice) the responsible department or Public Agency shall attempt to collect again by notifying the debtor by telephone and in writing that payment is now 30 days overdue and payable immediately.</p> <p>If payment is not received during the next 30 days (i.e., within 90 days of the date of the invoice) the overdue receivable becomes a delinquent account receivable. The responsible department or Public Agency shall:</p> <p>attempt to collect again by notifying the debtor that payment is now 60 days overdue and payable immediately; and transfer collection responsibility to the Financial Reporting and Collections Section, Finance, immediately.</p>		<p>payment.</p> <p>FESS sends customer statements for all accounts receivable outstanding 30 days. The department reviews accounts receivable outstanding 30-90 days and makes collection efforts within the department by making phone calls to the customers.</p> <p>The collection responsibility is assigned correctly to the collections department at 90 days.</p>

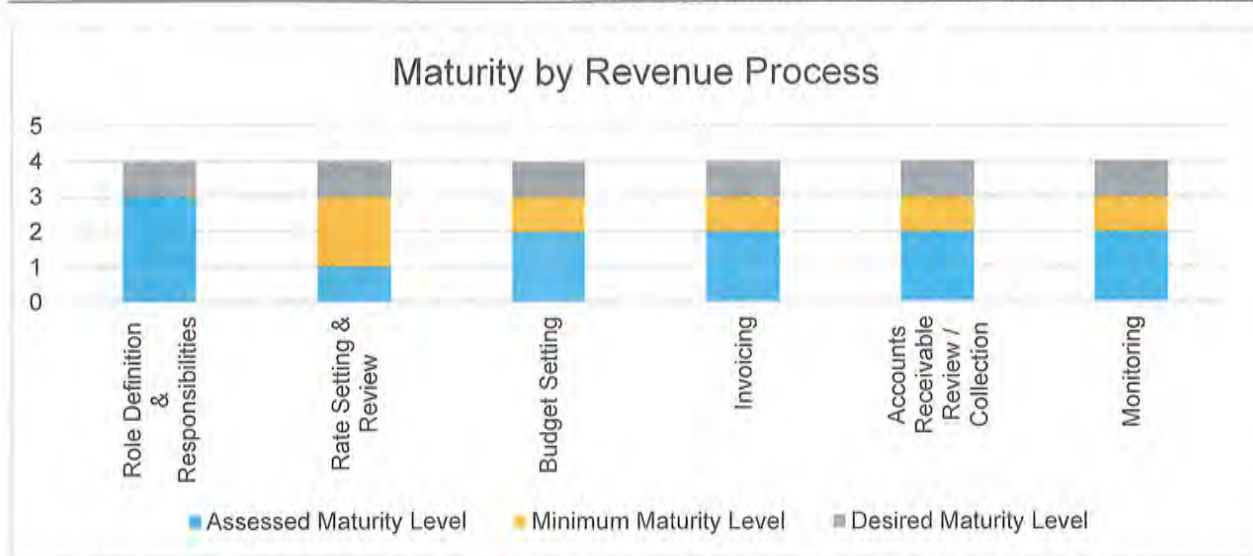
**Maturity Rating Considering GNWT Internal Control Capacity Model**

Using the GNWT Internal Control Capacity Model (**Appendix E**), the assessed maturity, minimum maturity and desired maturity are illustrated in the graph below.

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

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

**Desired Maturity Level** – This level would be achieved via long term goals (>24 months) and should be part of long term planning if applicable to your department. Desired maturity level has been set by Crowe at a level that is considered achievable over time by the department and taking into account the level of risk in the department.



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

Revenue Process Area	Assessed Maturity Level	Findings and Comments
<b>Role Definition and Responsibilities</b> The department defines, documents, communicates, and assigns accountability for its revenue processes and procedures. Roles are defined and responsibilities address all aspects of revenue.	Defined	<ul style="list-style-type: none"> <li>Job descriptions exist for the positions outlined above under departmental background as responsible for the department's general revenue functions.</li> <li>Job descriptions include responsibilities related to specific general revenue cycle components.</li> <li>Job descriptions reviewed by Crowe have all been updated within the last four years.</li> </ul>
<b>Rate Setting &amp; Review</b> The department reviews rates on a set periodic basis to ensure rates are current and new revenue sources have been considered.	Ad Hoc	<ul style="list-style-type: none"> <li>Majority of rates and fees are regulated and are charged in accordance with regulations.</li> <li>Regulated rates and fees are reviewed every five years as per FMB direction.</li> <li>Non-regulated rates and fees are not reviewed on a set periodic basis, and policies and processes are not documented.</li> <li>New sources of revenue are considered when new programs or initiatives are planned but a formal process does not exist.</li> <li>Rate rationale has not been documented.</li> </ul> <p><i>See Observation 1, 2 and 3.</i></p>
<b>Budget Setting</b> The department clearly defines and documents the revenues expected for each year with explanations for any material changes from prior years.	Repeatable	<ul style="list-style-type: none"> <li>Clarity on roles and responsibilities exists for ENR Financial Planning.</li> <li>ENR Financial planning prepares the operating budget with revenue estimates from Corporate Services.</li> </ul>

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> <li>Budget of revenues is based on prior year estimates and actuals with input from program managers not on statistical information.</li> <li>Assumptions and rationale for estimates are not documented.</li> </ul> <p><i>See Observation 4.</i></p>
<p><b>Invoicing</b></p> <p>The department ensures that invoices are prepared in a timely manner, and are accurate and complete.</p>	Repeatable	<ul style="list-style-type: none"> <li>Invoices are not issued for the majority of the department's revenue streams because payment is received at the time of service, or the revenue is from self-reporting by vendors.</li> <li>Processes are in place to record revenues received in cash or by online payment at the time the service is provided.</li> <li>Processes are in place to ensure all revenues earned are recorded as revenues for revenues received by cheque or direct payment.</li> <li>Processes are not fully documented for each revenue stream.</li> </ul> <p><i>See Observation 5.</i></p>
<p><b>Accounts Receivable Review / Collection</b></p> <p>The department monitors receivables on a set periodic basis and ensures that follow-up takes place if revenues are not received as expected.</p>	Repeatable	<ul style="list-style-type: none"> <li>The department has a "Finance General" email established for emails from FESS and a department representative has been assigned.</li> <li>The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque.</li> <li>The department's process for addressing emails received from FESS is not documented.</li> <li>The process the department has for addressing emails received from FESS regarding unallocated receipts by cheque does not include specific procedures to be taken by department staff.</li> <li>The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting.</li> <li>The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting.</li> <li>The procedures to be taken when an unclaimed deposits email is received from Department of Finance - Financial Reporting have not been established and documented.</li> <li>Accounts receivable are reviewed monthly in accordance with the SAM Month End Checklist and actions are taken within department to follow-up on balances outstanding between 30 and 90</li> </ul>

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		days. <ul style="list-style-type: none"> <li>“On Account” balances in the department’s accounts receivable are reviewed at least two times per year by Corporate Services, which includes interaction with FESS, but per review of credit AR balances, there are items outstanding which are coded to the department.</li> <li>The department understands the role and responsibility of the Collections unit.</li> </ul> See Observations 6, 7, 8 and 9.
<b>Monitoring</b> The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are not being received as expected.	Repeatable	<ul style="list-style-type: none"> <li>Monthly and quarterly variances are prepared by Financial Planning based on budgeted revenues versus actuals revenues per reports from SAM.</li> <li>Explanations for variances are documented.</li> <li>Variance reports are reviewed and provided to Management Board Secretariat.</li> <li>Process for variance analysis is not documented.</li> </ul> See Observation 10.

## OBSERVATIONS AND RECOMMENDATIONS

### Observation 1

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

- Although regulated rates and fees are reviewed every five years per FMB direction, documentation of fee review is lacking and rationale for fee changes is not documented.
- The department informally reviews non-regulated rates and fees but policy and process around these have not been documented.

#### Risk Profile:

Risk Impact	Without clearly documented processes for review of legislation and rates, fees may not be adequate to cover related costs.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

#### Recommendations:

We recommend that:

- For each revenue stream and type of rates, and the process established to review rates and fees, should be evaluated to ensure the activities required occur on a set periodic basis that adequately address economical changes which would impact the rate and fee; the process should be documented including roles and responsibilities.

#### Management Response:

Action Plan	Completion Date:
a) ENR is in the process of designing	June 30, 2019



<p>procedures to ensure that the established policies and processes for reviewing rates and fees are documented and evaluated on a regular basis as required by FAM.</p> <p>Staff members responsible for each revenue stream will take the lead of documenting the policies and processes for rates and fees. They will be assisted by Corporate Services Division.</p>	
--	--

### Observation 2

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

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

#### Risk Profile:

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

#### Recommendations:

We recommend that:

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

#### Management Response:

Action Plan	Completion Date:
<ol style="list-style-type: none"> <li>ENR is in the process of documenting the process involved in setting &amp; reviewing the rates.  Staff members responsible for each revenue stream will document the rationale for the rate as it was explained to the auditors</li> </ol>	June 30, 2019

### Observation 3

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

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

#### Risk Profile:

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

Risk Mitigation Support	Manager, Corporate Services
-------------------------	-----------------------------

**Recommendations:**

We recommend that:

- a) A policy should be formalized that requires revenues to be considered for all new programs or initiatives at the planning stage, including maintenance of records to substantiate decisions made.

**Management Response:**

Action Plan	Completion Date:
a) The Department is in the process of documenting the procedures to be taken to assess potential new revenue.	June 30, 2019

**Observation 4**
**Basis of budgeted revenues is not fully documented.**

- General revenues of the department are consistent from year-to-year, as such, budgeted revenues are based on prior year estimates and actuals with input from program managers. Balances with changes from prior years are explained, but those without are not.
- General revenue budgets are not based on statistical information and assumptions and rationales are not fully documented.

**Risk Profile:**

Risk Impact	A lack of documentation of explanations for unchanged budgeted amounts indicates that analysis and review of the revenues has not been made.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- a) Statistical information be used, where possible, and assumptions and explanations for budgeted revenues be documented for each significant general revenue source.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in the process of adding more statistical tools in analyzing revenue stream. This will be done through the monthly variances.	June 30, 2019

**Observation 5**
**Revenue processes are not fully documented.**

- Processes are in place for each revenue stream to ensure revenues earned are recorded but are not documented.
- Environment Fund processes are documented and have been reviewed and updated within the past 12 months but do not include the processes in place to ensure all revenues earned are recorded.

**Risk Profile:**

Risk Impact	Without documented revenue policies and procedures, consistent direction cannot be given to departmental personnel, and consistent application may not occur, which could result in earned revenues not being recorded and receipts not being collected.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- a) Revenue policies and processes in place should be fully documented for each significant revenue stream and should include roles and responsibilities, how revenues are initiated and recorded, and the controls in place to ensure all revenues earned are recorded.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in the process of documenting the procedures followed in initiating revenue recording controls in place, and ensuring all ENR revenue earned is recorded and in the correct period.	June 30, 2019

**Observation 6**

**Process for addressing unallocated cheque emails from FESS is not documented and the process lacks procedures to be performed.**

- The department representative, Manager, Corporate Services, for the "Finance General" email account forwards emails received from FESS for unallocated cheques to the applicable department staff for review. FESS sends an email when a cheque has been received that cannot be allocated and the department is given 48 hours to reply.
- If the cheque is identified by department staff as being for ENR and the purpose of the receipt is known, the department staff will email the department representative and the department representative will email FESS with instructions on how to apply the receipt.
- The process is not documented and specific procedures to be taken by department staff upon receipt of an email for an unallocated cheque from the department representative has not been designed and documented.

**Risk Profile:**

Risk Impact	Without specific procedures being designed and documented it may be unclear to staff what should be done when an unallocated cheque email is received, which could result in no action being taken or insufficient action taken. This increases the risks of lost revenue to the department or incorrectly recorded receipts "On Account" to the department. Without a documented process, consistent direction cannot be given to departmental staff, and verbally communicated processes may not be transferred to new staff.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- a) Procedures should be designed to ensure all possible actions are taken by department staff for unallocated cheques received by FESS.
- b) Processes and procedures should be documented regarding the receipt of unallocated cheque emails from FESS.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in the process of documenting procedures of handling unallocated funds from FESS.  The new procedures will be shared with all concerned staff members and also stored in DIIMS.	June 30, 2019
b) ENR is in the process of designing and documenting procedures of handling the emails received from FESS in relation to unallocated funds.  The new procedures will be shared with all concerned staff members and also stored in DIIMS.	June 30, 2019

**Observation 7**
**Process for direct payment notifications received by department staff is not documented.**

- When a direct payment notification is received by department staff, the notification is to be forwarded to Department of Finance – Financial Reporting with details of how the payment should be applied.
- The process is not documented and the information to be sent to Financial Reporting with the direct payment notification has not been clearly defined.

**Risk Profile:**

Risk Impact	Without a documented process, consistent direction cannot be given to departmental staff and verbally communicated processes may not be transferred to new staff. Inconsistent application of the process increases the risk that ENR revenues will be unrecorded.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- a) A process for handling direct payment notifications received by department staff should be documented and should identify the information to be provided to Financial Reporting in addition to the direct payment notification.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in the process of designing and documenting procedures for handling direct payment notifications to ensure they are communicated to Financial Reporting with the correct supporting information.  The new procedures will be shared with all concerned staff members and also stored in DIIMS.	June 30, 2019

**Observation 8**
**Process for addressing unclaimed deposit emails from Financial Reporting is not documented and the process lacks procedures to be performed.**

- The Manager, Corporate Services, receives all emails from Financial Reporting for unclaimed deposits (direct payments received for which the purpose has not been determined by Financial Reporting).
- The email received is forwarded by Manager, Corporate Services, to the applicable department staff for review.
- If a payment is identified by department staff as being for ENR and the purpose of the receipt is known the department staff will email the Manager, Corporate Services, with the coding.
- The Manager, Corporate Services, provides the information received to Financial Reporting with instructions on how to apply the receipt.
- The process is not documented and specific procedures to be taken by department staff upon receipt of the unclaimed deposits email have not been designed and documented.

**Risk Profile:**

Risk Impact	Without specific procedures being designed and documented it may be unclear to staff what should be done when an unclaimed deposit email is received which could result in no action being taken, or insufficient action taken, which could cause lost revenue to the department.  Without a documented process, consistent direction cannot be given to departmental staff, and verbally communicated processes may not be transferred to new staff.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- Procedures should be designed to ensure all possible actions are taken by department staff for unclaimed deposits identified by Financial Reporting, and ensure the actions taken are timely.
- Processes and procedures should be documented to address unclaimed deposit emails from Financial Reporting.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in the process of designing and documenting procedures of identifying unclaimed deposits provided to the	May 31, 2019

department by Financial Reporting. The new procedures will be shared with all concerned staff members and also stored in DIIMS.	
b) ENR is in the process of designing and documenting procedures of handling the emails received from Financial Reporting in relation to unclaimed deposits.  The new procedures will be shared with all concerned staff members and also stored in DIIMS.	May 31, 2019

### Observation 9

#### Processes have not been documented to address "On Account" accounts receivable.

- When FESS receives cheques for revenues/accounts receivable for which the department is known, yet the purpose is unknown, FESS sends an email to the "Finance General" email of the department asking for instructions on how to process the cheque.
- If a response is not received from the department, the receipt of the cheques is recorded to the customer and department "On Account" which creates a credit balance in the department's accounts receivable listing.
- As at December 30, 2018, ENR's accounts receivable included \$92,720 of "On Account" credit balances from 2014/15 fiscal year to 2018/19 fiscal year, broken down as follows:
  - 2014/15 fiscal \$63,716
  - 2015/16 fiscal \$11,641
  - 2016/17 fiscal \$6,985
  - 2017/18 fiscal \$6,944
  - 2018/19 fiscal \$3,435
- Although processes for review are in place, a formal process has not been documented to review "On Account" accounts receivable by the department on a regular basis.

#### Risk Profile:

Risk Impact	Without a process being documented, "On Account" receivables may not be fully addressed and department revenue can go unrecorded. The longer the passage of time between the receipt and review of the receipt, the more difficult it becomes to identify the purpose of the receipt and ensure it is applied appropriately.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

#### Recommendations:

We recommend that:

- a) A formal process should be documented that ensures "On Account" receivables are reviewed monthly
- b) Explanations should be provided for any outstanding "On Account" balances existing for more than 30 days.

#### Management Response:

Action Plan	Completion Date:
a) ENR is in the process of documenting the current procedures taken to review Accounts Receivable credit balances.	June 30, 2019

b) This process is done on a monthly basis. Any outstanding balances over 30 days in "On Account" Receivables will be explained. In addition to a submission provided to Financial Reporting & Collection for Year end.	June 30, 2019
---	---------------

**Observation 10**
**Variance analysis preparation process has not been documented.**

- Variance analysis is performed monthly and quarterly with variance explanations provided. Roles and responsibilities of variance analysis preparation are known, but the process is not fully documented.

**Risk Profile:**

Risk Impact	Without a documented variance analysis process, consistent direction cannot be given to departmental personnel responsible for the process should personnel changes occur.
Risk Responsibility	Director, Environment and Natural Resources, Corporate Services
Risk Mitigation Support	Manager, Corporate Services

**Recommendations:**

We recommend that:

- The variance analysis process should be fully documented including roles and responsibilities of department staff as well as timelines.

**Management Response:**

Action Plan	Completion Date:
a) ENR is in process of documenting the Variance Analysis procedures	June 30, 2019

GNWT Revenue Process Audit  
Roles & Responsibilities

Appendix A

**Financial Administration Manual**

	Department	Financial Reporting / Collections	MBS / FMB	Comptroller General
<b>Establishment of Fees</b>	<ul style="list-style-type: none"> <li>Deputy Head responsible to set fees and charge for licenses, permits and services rendered to the public</li> <li>Minister responsible to advise the FMB of the introduction, change or removal of a fee within 60 days</li> </ul>	-	MBS may issue directives respecting financial management or administration of a Public Agency	<ul style="list-style-type: none"> <li>May approve Interpretation Bulletins associated with this policy</li> <li>Establish and maintain systems and procedures to ensure the integrity of GNWT financial records and accounting systems</li> <li>Establish/ maintain systems and procedures to ensure public money is collected and accounted for, internal controls are in place</li> </ul>
<b>Rationale for Fees Charged</b>	<ul style="list-style-type: none"> <li>Ensure fees are collected, safeguarded, and accounted for</li> <li>Rationale for each fee must be kept for audit purposes</li> </ul>	-	-	
<b>Recording Revenue</b>	<ul style="list-style-type: none"> <li>Deputy Head of dept. responsible to ensure revenues accurately recorded in a timely manner in accordance with GAAP</li> </ul>	-	-	
<b>Receipt of money</b>	<ul style="list-style-type: none"> <li>Responsible for collection and management of all A/R</li> </ul>	Engage courts or outside collection agency	-	



## GNWT Revenue Process Audit Roles & Responsibilities

### Appendix B

### Shared Services Agreement

	Department	FESS	Financial Reporting / Collections	MBS / FMB	SAM Team	Comptroller General
<b>Estimates (Budgets)</b>	• Prepare	-	-	• MBS review/ FMB approval	• Support	<ul style="list-style-type: none"> <li>• Appointed by Minister of Finance</li> <li>• Maintain systems and procedures with respect to the integrity of government financial records and accounting systems</li> <li>• Ensure compliance by GNWT departments, Public Agencies and other reporting bodies with accounting policies and practices</li> <li>• Manage Consolidated Revenue Fund and Public Accounts.</li> </ul>
<b>Variance reports</b>	• Prepare	-	-	• MBS review/ quarterly to FMB	• Support	
<b>Invoices</b>	• Request/ set up	• Acct. approval	-	-	• Maint.	
<b>Cash Payment</b>	• Process in- dept. receipts	• Process all other receipts	-	-	• System support	
<b>Cheque Payment</b>	• Provide coding	• Process/ post	-	-	• System support	
<b>EFT Payment</b>	• Provide invoice/ coding	• Post	• Process	-	• System support	
<b>A/R Mgmt</b>	• Follow-up <90 days; monitoring ongoing	• Stmt. sent to customer	• Follow-up >90 days; external collections; court	-	• System support	
<b>Training</b>	• Dept. training	• FESS training	• FR/ collection training	• MBS training	• SAM- based training	


Acronyms used in the charts below and further into the report are as follows:

Financial Employees Shared Services  
 Financial Management Board:  
 Management Board Secretariat:  
 System for Accountability and Management

FESS  
 FMB  
 MBS  
 SAM

## **APPENDIX C**

### **INTERNAL CONTROL CAPACITY MODEL**

 <b>Northwest Territories</b>	Effective Date: June 24, 2014	Section Title: Policy Framework and Standards	Section Number: 100
	Chapter Title: Internal Control and Risk Framework		Chapter Number: 150
	Task Title: Internal Control Capacity Model		Task Number: 153

Deliverable	Description
0 - Non-existent	<ul style="list-style-type: none"> <li>The organization lacks procedures to monitor the effectiveness of internal controls.</li> <li>Management internal control reporting methods are absent.</li> <li>There is a general unawareness of internal control assurance.</li> <li>Management and employees have an overall lack of awareness of internal controls.</li> </ul>
1 - Initial/Ad Hoc - Unreliable	<p>Unpredictable environment for which controls have not been designed or implemented.</p> <ul style="list-style-type: none"> <li>Controls are fragmented and ad hoc.</li> <li>Controls are generally managed in silos and reactive.</li> <li>Lack of formal policies and procedures.</li> <li>Dependent on the "heroics" of individuals to get things done.</li> <li>Higher potential for errors and higher costs due to inefficiencies.</li> <li>Controls are not sustainable.</li> <li>Individual expertise in assessing internal control adequacy is applied on an ad hoc basis.</li> <li>Management has not formally assigned responsibility for monitoring the effectiveness of internal controls.</li> </ul>
2 - Repeatable - Informal	<p>Controls are present but inadequately documented and largely dependent on manual intervention. There are no formal communications or training programs related to the controls.</p> <ul style="list-style-type: none"> <li>Controls are established with some policy structure.</li> <li>Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan.</li> <li>Formal process documentation is still lacking.</li> <li>Some clarity on roles and responsibilities, but not on accountability.</li> <li>Increased discipline and guidelines support repeatability.</li> <li>High reliance on existing personnel creates exposure to change.</li> <li>Internal control assessment is dependent on the skill sets of key individuals.</li> </ul>
3 - Defined - Standardized	<p>Controls are in place and documented, and employees have received formal communications about them. Undetected deviations from controls may occur.</p> <ul style="list-style-type: none"> <li>Controls are well-defined and documented, thus there is consistency even in times of change.</li> <li>Overall control awareness exists.</li> <li>Policies and procedures are developed for assessing and reporting on internal control monitoring activities.</li> <li>A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers.</li> <li>Control gaps are detected and remediated timely.</li> <li>Performance monitoring is informal, placing great reliance on the diligence of people and independent audits</li> </ul>

Deliverable	Description
	<ul style="list-style-type: none"> <li>• Management supports and institutes internal control monitoring.</li> <li>• An education and training program for internal control monitoring is defined.</li> <li>• Tools are being utilized but are not necessarily integrated into all processes.</li> </ul>
4 - Managed - Monitored	<p>Standardized controls are in place and undergo periodic testing to evaluate their design and operation; test results are communicated to management. Limited use of automated tools may support controls.</p> <ul style="list-style-type: none"> <li>• Key Performance Indicators (KPIs) and monitoring techniques are employed to measure success.</li> <li>• Greater reliance on prevention versus detection controls.</li> <li>• Strong self-assessment of operating effectiveness by process owners.</li> <li>• Chain of accountability exists and is well-understood.</li> <li>• Management implements a framework for internal control monitoring.</li> <li>• A formal internal control function is established, with specialized and certified professionals utilizing a formal control framework endorsed by senior management.</li> <li>• Skilled staff members are routinely participating in internal control assessments.</li> <li>• A metrics knowledge base for historical information on internal control monitoring is established.</li> <li>• Peer reviews for internal control monitoring are established.</li> <li>• Tools are implemented to standardize assessments and automatically detect control exceptions.</li> </ul>
5 - Optimized	<p>An integrated internal controls framework with real-time monitoring by management is in place to implement continuous improvement. Automated processes and tools support the controls and enable the organization to quickly change the controls as necessary.</p> <ul style="list-style-type: none"> <li>• Controls are considered "word class", based on benchmarking and continuous improvement.</li> <li>• The control infrastructure is highly automated and self-updating, thus creating a competitive advantage.</li> <li>• Extensive use of real-time monitoring and executive dashboards.</li> <li>• Management establishes an organization wide continuous improvement program that takes into account lessons learned and industry good practices for internal control monitoring.</li> <li>• The organization uses integrated and updated tools, where appropriate, that allow effective assessment of critical controls and rapid detection of control monitoring incidents.</li> <li>• Benchmarking against industry standards and good practices is formalized.</li> </ul>

### Initial

- internal controls are fragmented and ad hoc
- generally managed in silos and reactive
- lack of formal policies and procedures
- dependent on the “heroics” of individuals to get things done
- higher potential for errors
- higher costs due to inefficiencies
- not sustainable

### Repeatable

- internal controls are established with some policy structure
- formal process documentation still lacking
- some clarity on roles, responsibilities and authorities, but not accountability
- increased discipline and guidelines support repeatability
- high reliance on existing personnel creates exposure to change

### Defined

- internal controls are well defined and documented, thus there is consistency even in times of change
- overall control awareness exists
- internal control gaps are detected and remediated timely
- performance monitoring is informal, placing great reliance of people and independent audits

### Managed

- Key performance indicators and monitoring techniques are employed to measure success
- greater reliance on prevention versus detection controls
- strong self assessment of operating effectiveness by process owners
- chain of accountability exists is well understood

### Optimized

- internal controls are considered “world class,” based on benchmarking and continuous improvement
- the internal control infrastructure is highly automated and self-updating, thus creating a competitive advantage
- extensive use of real-time monitoring and executive dashboards