



MAY 30 2018

CONFIDENTIAL

File: 7820-20-GNWT-151-131

MR. DAVID STEWART
DEPUTY MINISTER AND SECRETARY TO THE FMB
FINANCE

Access to Information and Protection of Privacy Assessment

Enclosed is the above referenced Assessment.

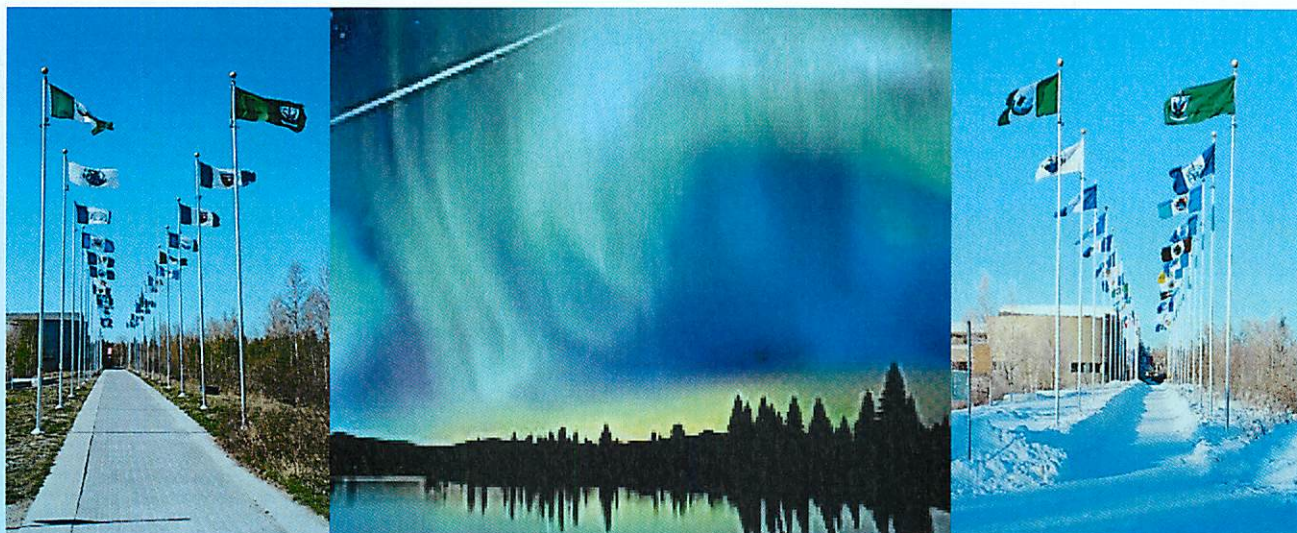
We will schedule a follow-up in the future to determine the progress of the agreed upon Management Action Plan. However, we would appreciate an update by November 2018 on the status of the management action plan.

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

T. Bob Shahi
Director, Internal Audit Bureau
Finance

Enclosure

- c. Mr. Jamie Koe, Chair, Audit Committee
Mr. Terence Courtoreille, Director, Corporate Affairs, Finance



FINANCE

Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018



FINANCE

Access to Information and Protection of Privacy Assessment

May 2018

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



CONFIDENTIAL

May 30, 2018

File: 7820-20-GNWT-151-131

MR. DAVID STEWART
DEPUTY MINISTER AND SECRETARY TO THE FMB
FINANCE

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 Finance was part of the GNWT wide audit project. This report identifies issues specific to your department.

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

B. BACKGROUND

The 1996 *ATIPP Act* plays a critical part in maintaining government accountability and protecting the public's personal information. The legislation

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

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

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

C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

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

The contractor assessed the compliance to *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 “high” requiring internal control capacity at “managed” level. The current capacity of the department was at the “ad-hoc”, meaning that processes were primarily dependent on individuals getting things done. The immediate task for the department was to develop systematic privacy processes and then focus on documenting the privacy process (defined level). Subsequently, the department can focus on identifying and addressing 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 Finance be advised on 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.

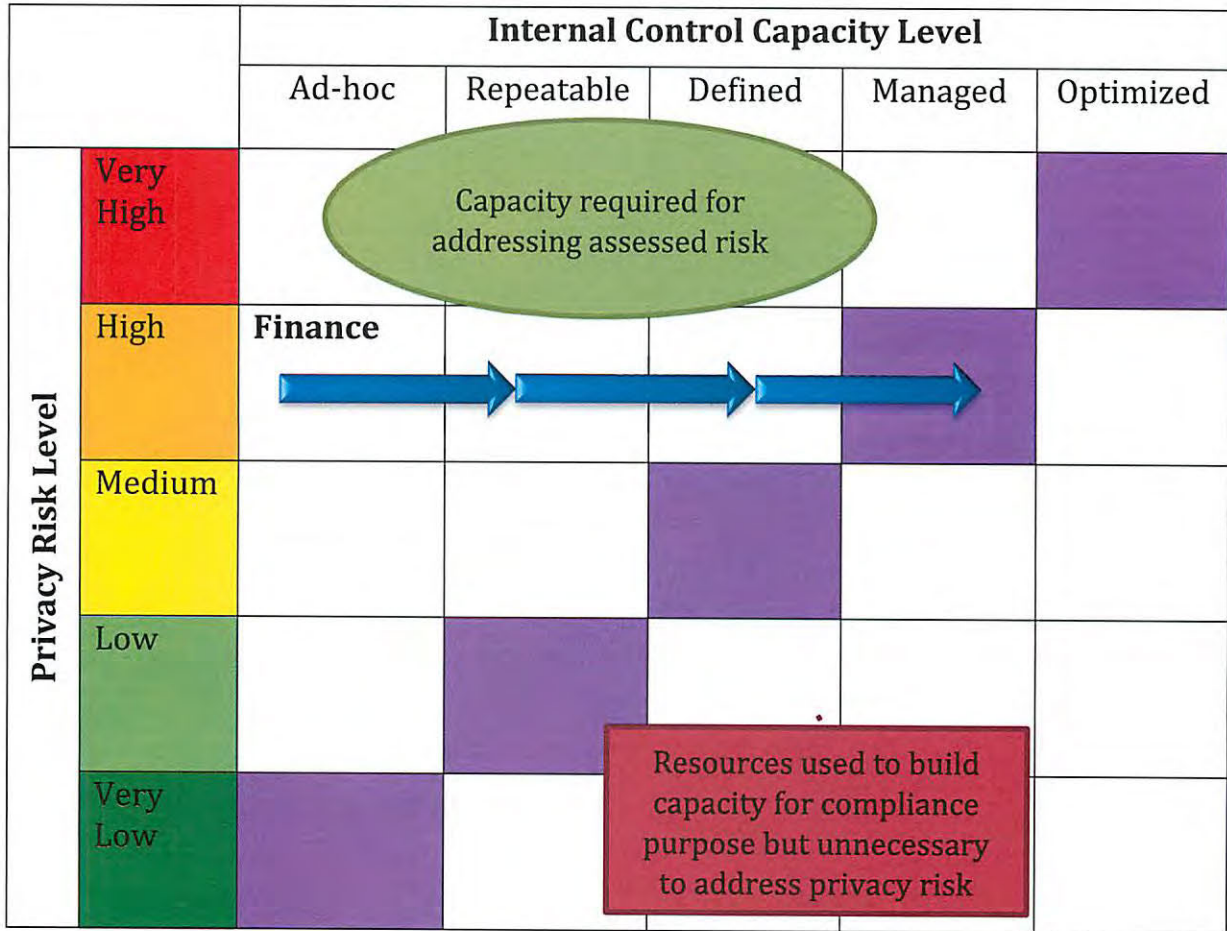


T. Bob Shahi
Director, Internal Audit Bureau
Finance

Chart I

Risk and Opportunity Assessment using Capacity Model

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



DEPARTMENT OF FINANCE

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

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

Finance collects personal information through:

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

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

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

DEPARTMENT OF FINANCE

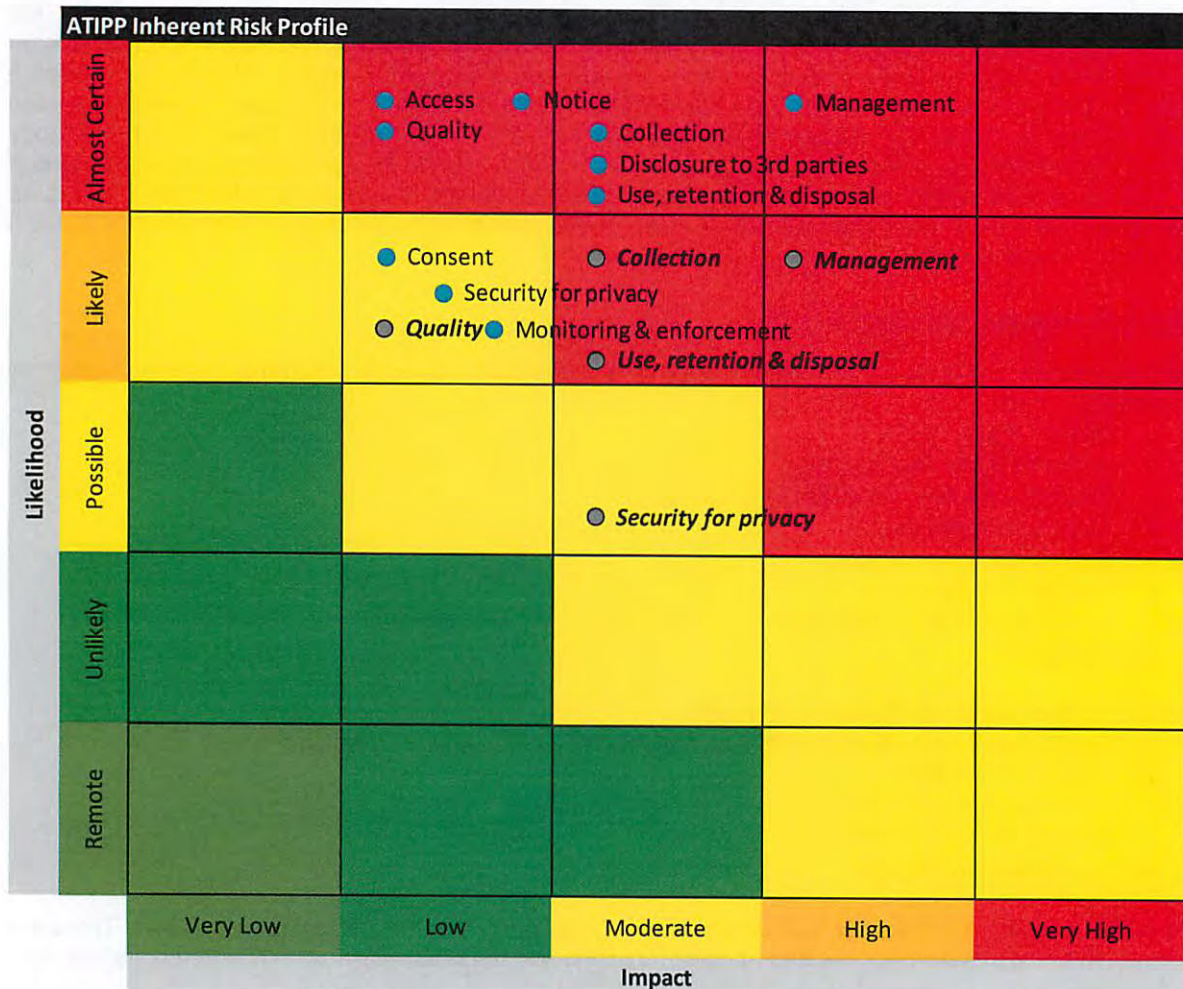
ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT (ATIPP) (PART 2)

Overview

Risk Profile

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

RISK HEATMAP



DEPARTMENT OF FINANCE

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

Compliance with ATIPP Part 2 Protection of Privacy

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

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

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

Maturity Rating against Privacy Maturity Model

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

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

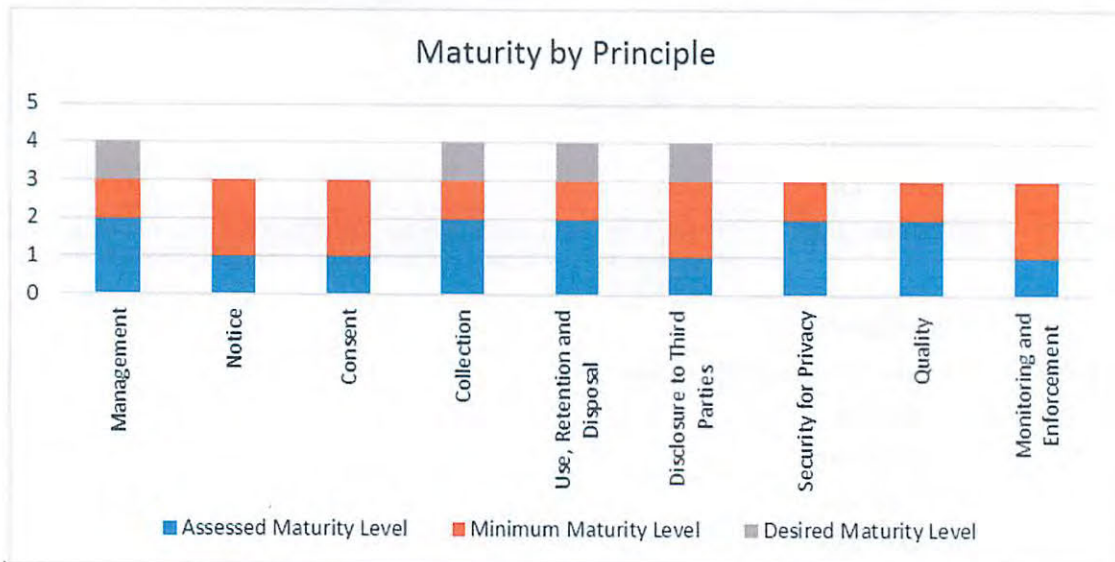
Minimum Maturity Level – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

DEPARTMENT OF FINANCE

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

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

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



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

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

DEPARTMENT OF FINANCE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> Privacy Impact Assessments are performed when needed and management works to ensure there is a culture which supports privacy compliance due to the highly confidential nature of the data they work with. <p><i>See observations 1-2.</i></p>
<p>Notice</p> <p>The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address notice to individuals. Notice is not provided on all forms used to collect personal information. <p><i>See observation 3.</i></p>
<p>Consent</p> <p>The department describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address consent of individuals. Implicit consent is obtained on some personal information collection forms but not all. Explicit consent is not obtained. <p><i>See observation 4.</i></p>
<p>Collection</p> <p>The department collects personal information only for the purposes identified in the notice</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address collection of personal information. Collection of information is limited to the intended use per the use of very detailed forms that request very specific information. A procedure/process does not exist to ensure only information needed is collected. Information obtained by third parties is rare, and when received is disclosed to individual in question <p><i>See observation 1.</i></p>
<p>Use, retention and disposal</p> <p>The department limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address use, retention and disposal. A procedure/process does not exist to ensure information collected is only used for the purpose it was collected for. Retention and disposal of information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the Digital Integrated Information Management System (DIIMs) which allows for

DEPARTMENT OF FINANCE

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

Generally Accepted Privacy Principle	Assessed Maturity Level	Findings and Comments
		<p>information to be retained for no longer than necessary and is disposed of at that time.</p> <ul style="list-style-type: none"> Information not yet stored in DIIMs is fully managed within other programs with existing use/disposal schedules. <p><i>See observation 1.</i></p>
<p>Disclosure to third parties</p> <p>The department discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</p>	Ad Hoc	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be taken if the information was misused by the third party. Information sharing agreements 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. <p><i>See observation 6.</i></p>
<p>Security for privacy</p> <p>The department protects personal information against unauthorized access (both physical and logical).</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address security for privacy. 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. Logical access to personal information is restricted by the department through the use of DIIMS and database restrictions put in place. Physical access to personal information is restricted via close off working spaces and use of locked cabinets for sensitive information. Security measures exist over the transmission of data but are not formally designed and documented. Tests of safeguards in place are not performed. <p><i>See observation 1.</i></p>
<p>Quality</p> <p>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice.</p>	Repeatable	<ul style="list-style-type: none"> A privacy policy has not been formally designed and documented to address quality to ensure personal information is complete and accurate for the purposes for which it is to be used and it is relevant to the purposes for which it is to be used.

DEPARTMENT OF FINANCE

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

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

Observations and Recommendations

Observation 1

Privacy policy has not been designed and documented

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
	Fall 2018

DEPARTMENT OF FINANCE

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

<p>Agreed. The Department of Finance will develop departmental level processes and procedures in conjunction with the development of a GNWT-wide privacy policy and guidelines.</p> <p>Action: Develop Department of Finance-specific privacy process and procedures to compliment the GNWT-wide privacy policy and guidelines</p>	
--	--

Observation 2

An inventory of personal information collected does not exist

- Department staff have knowledge of the personal information collected and are able to track the information that is most sensitive by employee name and number, but a full inventory has not been documented.
- Systems involved in collection and storage of personnel information are not documented.
- Third parties involved are not identified and documented.

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
<p>Confirmed. The Department will create an inventory of all types of personal information collected to be held by the ATIPP Coordinator. A further review of this inventory will be completed to ensure compliance with the Policy, guidelines and procedures identified in Response #1 above.</p> <p>Action:</p> <ul style="list-style-type: none"> a. Develop inventory of personal information collected. b. Review inventory to ensure compliance with policy, guidelines and procedures. 	<p>Fall 2018</p> <p>Fall 2018</p>

DEPARTMENT OF FINANCE

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

Observation 3

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

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

Observation 4

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

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

Risk Profile:

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

DEPARTMENT OF FINANCE

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

Recommendations:

We recommend that:

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

Management Response:

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

Observation 5

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

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

DEPARTMENT OF FINANCE

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

Observation 6

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

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

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

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 or call (978) 750-8400.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA

Vice Chair

Kenneth D. Askelson, CPA, CITP, CIA

Eric Federing

Philip M. Juravel, CPA, CITP

Sagi Leizerov, Ph.D., CIPP

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

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

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

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

Staff Contacts:

Nicholas F. Cheung, CA, CIPP/C

CICA

Principal, Guidance and Support

and

Nancy A. Cohen, CPA, CITP, CIPP

AICPA

Senior Technical Manager, Specialized Communities and Practice Management

Appendix A

AICPA/CICA Privacy Maturity Model

Acknowledgements

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



Table of Contents

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

Appendix A

AICPA/CICA Privacy Maturity Model

This page intentionally left blank.

AICPA/CICA Privacy Maturity Model User Guide

1 INTRODUCTION

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

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

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

2 AICPA/CICA PRIVACY RESOURCES

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

Generally Accepted Privacy Principles (GAPP)

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

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

The ten principles that comprise GAPP:

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

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

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

Privacy Maturity Model

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

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

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

The PMM uses five maturity levels as follows:

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

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.

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

Getting Started

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

Start-up activities could include:

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

Document Findings against GAPP

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

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

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

Assessing Maturity Using the PMM

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

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

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

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

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

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

5 PRIVACY MATURITY MODEL REPORTING

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

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

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

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

Figure 1 – Privacy Maturity Report by GAPP Principle

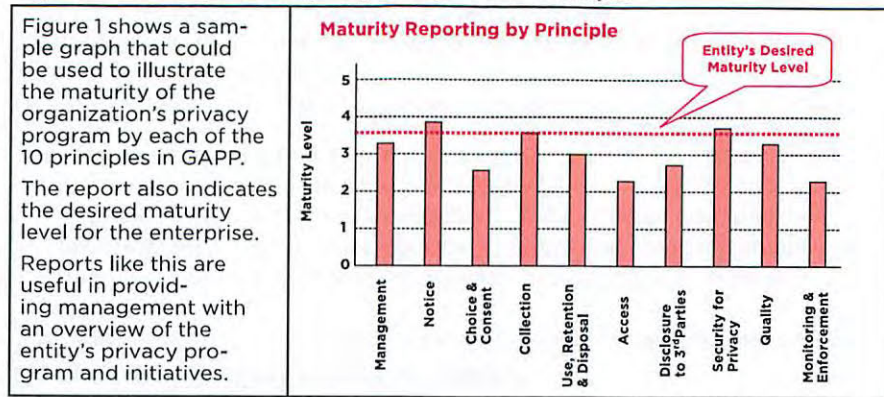


Figure 2 – Maturity Report by Criteria within a Specific GAPP Principle

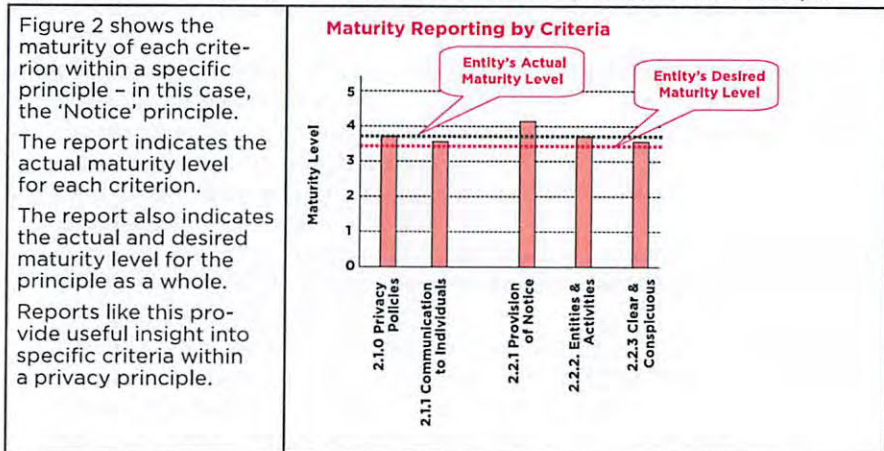
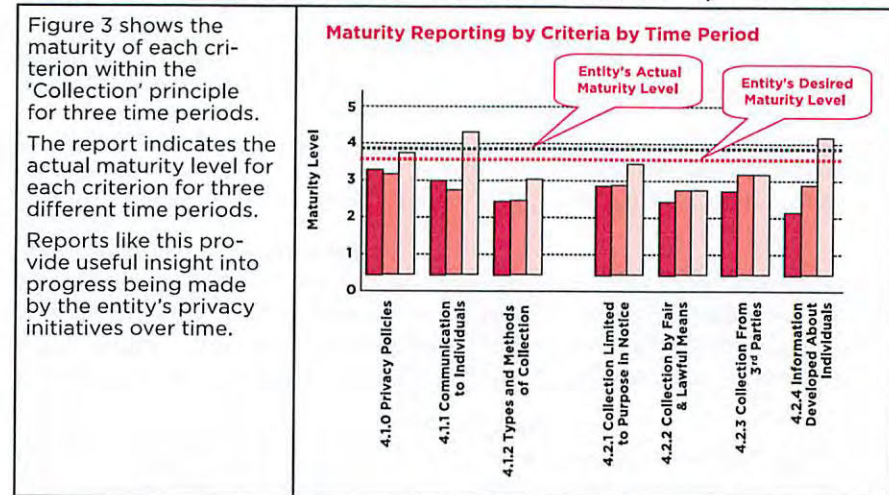


Figure 3 – Maturity Report by Criteria within a GAPP Principle Over Time



6 SUMMARY

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

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

AICPA/CICA PRIVACY MATURITY MODEL¹

Based on Generally Accepted Privacy Principles (GAPP)²

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

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

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

GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Logical Access Controls (8.2.2)	<p>Logical access to personal information is restricted by procedures that address the following matters:</p> <ul style="list-style-type: none"> a. Authorizing and registering internal personnel and individuals b. Identifying and authenticating internal personnel and individuals c. Making changes and updating access profiles d. Granting privileges and permissions for access to IT infrastructure components and personal information e. Preventing individuals from accessing anything other than their own personal or sensitive information f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities g. Distributing output only to authorized internal personnel h. Restricting logical access to offline storage, backup data, systems and media i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls) j. Preventing the introduction of viruses, malicious code, and unauthorized software 	<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
SECURITY FOR PRIVACY (9 criteria) cont.	The entity protects personal information against unauthorized access (both physical and logical).					
Physical Access Controls (8.2.3)	Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information).	Controls over physical access to personal information are informal, incomplete and inconsistent.	The entity has basic physical security procedures; however, they do not include specific requirements governing physical access to personal information maintained or stored in various media. Accordingly, inconsistent approaches are taken throughout the entity with respect to physically securing personal information.	The entity has implemented formal physical security policies and procedures that form the basis of specific privacy-related security procedures for physical access to personal information. Physical access to personal information is restricted to employees with a need for such access.	Management monitors physical access controls. Personal information is physically stored in secure locations. Access to such locations is restricted and monitored. Unauthorized access is investigated and appropriate action taken.	Where physical access or attempted violation of personal information has occurred, the events are analyzed and remedial action including changes to policies and procedures is adopted. This may include implementing increased use of technology, as necessary. Physical access controls are continually assessed and improved.
Environmental Safeguards (8.2.4)	Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	Some policies and procedures exist to ensure adequate safeguards over personal information in the event of disasters or other environmental hazards; however, they are incomplete and inconsistently applied. The entity may lack a business continuity plan that would require an assessment of threats and vulnerabilities and appropriate protection of personal information.	The entity has a business continuity plan addressing certain aspects of the business. Such a plan may not specifically address personal information. Accordingly, personal information may not be appropriately protected. Business continuity plans are not well documented and have not been tested.	The entity has implemented a formal business-continuity and disaster-recovery plan that address all aspects of the business and identified critical and essential resources, including personal information in all forms and media, and provides for specifics thereof. Protection includes protection against accidental, unauthorized or inappropriate access or disclosure of personal information. The plan has been tested.	Management monitors threats and vulnerabilities as part of a business risk management program and, where appropriate, includes personal information as a specific category.	Management risk and vulnerability assessments with respect to personal information result in improvements to the protection of such information.
Transmitted Personal Information (8.2.5)	Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry-standard encryption technology for transferring and receiving personal information.	The protection of personal information when being transmitted or sent to another party is informal, incomplete and inconsistently applied. Security restrictions may not be applied when using different types of media to transmit personal information.	Policies and procedures exist for the protection of information during transmittal but are not fully documented; however, they may not specifically address personal information or types of media.	Documented procedures that cover all relevant aspects have been implemented and are working effectively to protect personal information when transmitted.	The entity's policies and procedures for the transmission of personal information are monitored to ensure that they meet minimum industry security standards and the entity is in compliance with such standards and their own policies and procedures. Issues of non-compliance are dealt with.	Management reviews advances in security technology and techniques and updates their security policies and procedures and supporting technologies to afford the entity the most effective protection of personal information while it is being transmitted, regardless of the media used.

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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

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

Appendix A

AICPA/CICA Privacy Maturity Model

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



CONFIDENTIAL

November 10, 2017

File: 7820-20-GNWT-151-130

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

MR. DAVID STEWART
DEPUTY MINISTER
FINANCE

MR. TOM JENSON
DEPUTY MINISTER
INDUSTRY, TOURISM &
INVESTMENT

Management Letter: Business Incentive Policy (BIP) Awarded Contracts
Review Period: October 1, 2016 to August 30, 2017

The Audit Committee approved the project in the 2016-2017 Audit Work Plan. The risk assessment identified a gap in the evaluation of contract execution where contracts were awarded based on BIP adjustments (BIP Awarded Contracts).

The GNWT spends over \$250 million annually on contracts for goods and services. The BIP was established to:

- give preference on government procurement to NWT owned and operated businesses
- promote economic growth and capacity within NWT.

The audit objective was to determine if contractors were using NWT and/or local content in compliance with BIP Awarded Contracts.

In October 2016, the Internal Audit Bureau (IAB) began preliminary work to determine if clear direction was given to contractors and GNWT staff on the reporting requirements of BIP Awarded Contracts. The IAB gathered available BIP information from the Department of Industry, Tourism and Investment (ITI) and the GNWT's System for Accountability and Management (SAM) for contract, procurement and financial transactions.

As part of its preliminary work, the IAB noted the governance framework did not provide ITI clear direction to gather the relevant information required to monitor

and evaluate BIP Awarded Contracts. As such, the IAB could not easily trace the contract expenditures in SAM to determine how much local content was used into the BIP Awarded Contracts.

In May 2017, the IAB engaged the Director of Procurement Shared Services (Director) from the Department of Infrastructure (INF). The Director was aware of BIP's contract monitoring and evaluation issues. As a result, a BIP working group (Working Group) was created to draft the Financial Administration Manual 705-Procurement Interpretation Bulletin (FAM Bulletin). The BIP Senior Management Committee (BIP SMC), composed of Deputy Ministers of INF, ITI, Justice, Finance and NWT Housing Corporation, was responsible for reviewing and approving the FAM Bulletin.

On May 17, 2017 and June 1, 2017, the Working Group presented draft FAM Bulletin to the BIP SMC. The BIP SMC reviewed the proposed changes and requested additional information from the Working Group.

The IAB also reviewed and assessed the draft FAM Bulletin. The assessment indicated that the GNWT does not have sufficient authorization to request the required information to evaluate whether BIP Awarded Contracts are meeting the BIP objectives.

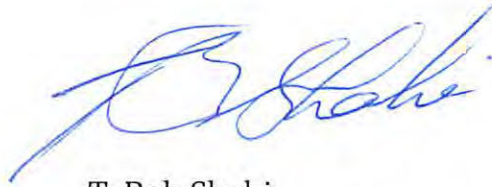
To monitor and evaluate the BIP objectives, the IAB recommends revising the policy, procedure and contracts terms to explicitly state mandatory requirements for:

1. Contractors to use NWT and/or local content
2. Contractors to provide the BIP registered businesses used and NWT and/or local labour content (name, address, payment amounts, etc.) **(Schedule I and II refers)** supported by a declaration form signed by a company senior executive
3. GNWT to monitor the impact of contractor non-compliance with the NWT and/or local content requirements
4. GNWT to assess the impact of contractor non-compliance and apply an appropriate remedial action, including holdback.

The IAB recognizes that a coordinated effort of Finance, ITI, and INF is required. As such, the IAB will follow up on management actions taken to update the governance process in 12 to 18 months. Once fully implemented, the IAB or an independent contractor could be engaged to provide an independent, objective assessment of the BIP Awarded Contract governance framework, information integrity and compliance.

We would like to thank the Director of Procurement Shared Services for his assistance and co-operation throughout this project.

Sincerely,



T. Bob Shahi
Director, Internal Audit Bureau

Enclosures

- c. Mr. Jamie Koe, Chair, Audit Committee
- Mr. Terence Courtoreille, Director, Corporate Affairs, Finance
- Mr. Vince McCormick, Director, Corporate Services, Infrastructure
- Ms. Julie Mujcin, Director, Finance & Administration, Industry, Tourism & Investment

Substantiation of Contractors use of NWT and/or local good and services

Contractor Name:
 Contract Ref. /PO #: XXXXXX
 Contract Term: April 1, 20XX to March 31, 20XX
 Reporting Period: April 1, 20XX to March 31, 20XX

	BIP Registry Name or Legal Name	Description of Goods and Services	Invoice #	Cheque #	Invoices Paid
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

GNWT reserves the right to audit information as stated in contract clause XX.

Statutory Declaration of Senior Executive (CEO, CFO):

Notary Public/ Commissioner:

Total Invoices Paid (above)	
Total Labour Paid [from Schedule II]	
Total Northern Amount Paid	
RFP/Tender quoted in BIP Contract:	
Variance:	

GNWT, BIP Awarded Contracts

File: 7820-21-GNWT-151-130

Schedule II

Substantiation of Contractors use of NWT and/or local labour

Contractor Name:

Contract Ref. /PO #: XXXXXX

Contract Term: April 1, 20XX to March 31, 20XX

Reporting Period: April 1, 20XX to March 31, 20XX

#	Employee name	Employee SIN #	Employee address	Date Hired	Date Terminated	Job Title	Number of hours worked	Amount Paid
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Total Labour Amount Paid [carry to Schedule I]:								



MAY 08 2019

File: 7820-20-GNWT-151-135

CONFIDENTIAL

MR. DAVID STEWART
DEPUTY MINISTER
FINANCE

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

A. SCOPE AND OBJECTIVES

The Audit Committee approved the operational audit of Government of Northwest Territories (GNWT) Revenue Process. The audit covered the complete revenue process of four GNWT departments from budgeting to variance analysis. The four departments were:

- Education, Culture & Employment
- Environment and Natural Resources
- Infrastructure
- Justice

This report summarizes the issues that affect more than one department as well as well the revenue process assigned to the Department of Finance (Finance).

B. BACKGROUND

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

- \$16 million in non-renewable resources
- \$77 million in general revenue
- \$251 million in taxation

According to FAM, the roles and responsibilities for establishing the fee, the fee rationale, recording, and receipt of money were allocated to departments, and various parts of Finance: Financial Reporting/Collection Services; Management Board Secretariat (MBS); and the Comptroller General.

.../2

Specific phases of GNWT revenue 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; MBS, and the Comptroller General.

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

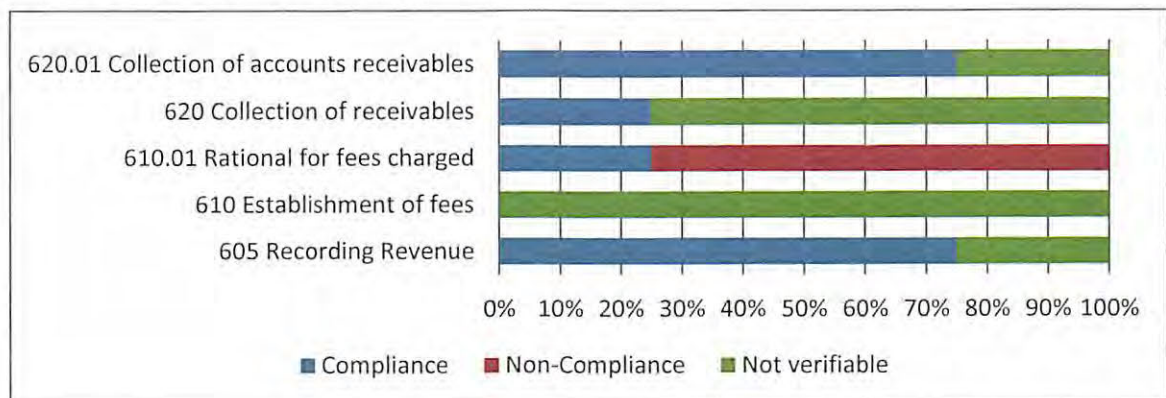
C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached audit report, *“Revenue Process Audit”* provides the details on the eight observations and the associated recommendations (**Schedule 1 refers**). The management responses to the recommendations have been incorporated in the attached report. Five additional observations by the contractor did not require recommendations.

Millions of dollars in GNWT generated revenue was processed monthly by departments and FESS in a timely fashion and allocated to the appropriate accounts.

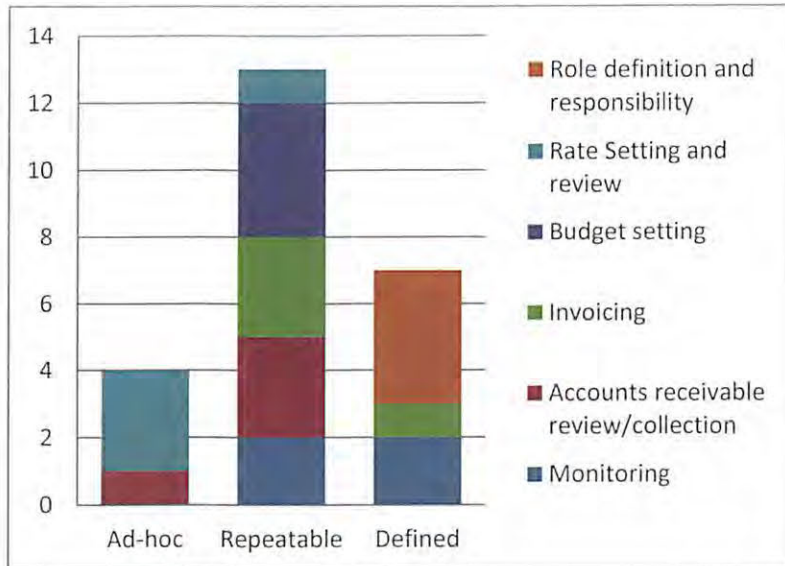
In reviewing the temporary account used for unallocated incoming revenue, the contractor observed that most of the \$14 million in the account was for Liquor Commission, payroll, and tax entries. A majority of the money was allocated to the appropriate areas except for over \$400,000 that had not been assigned for over ten months. The unassigned amounts ranged from a few pennies to over \$48,000 dating back to May 2014.

In assessing compliance with the FAM revenue requirements, the contractor identified a varying level of compliance:



The internal control capacity for the revenue processes varied in the four departments. The roles and responsibilities were well defined (all four department) while rate setting (three of four departments) was most at an ad-hoc level.

An internal control capacity at a defined level (rating of three of 5) was adequate to meet the needs of the four departments. A detailed risk assessment of revenue processes could identify a need for a more mature internal control capacity in specific areas.



Each department provided an independent response to the audit recommendations based on their own internal capacity. It is our view that the Office of the Comptroller General could take the lead in coordinating a collective action through the Director of Finance & Administration Committee. While only four departments were tested, it is highly likely that similar conditions exist in other departments. This is an opportune time for the first line (i.e. departments) to work with the second line (Office of the Comptroller General) to address the revenue processing risks. Risks that had been outstanding for number of years and to build internal control capacity.

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

D. ACKNOWLEDGEMENT

We would like to thank the department staff for their assistance and cooperation throughout the audit.

T. Bob Shahi
Director, Internal Audit Bureau
Finance

SCHEDULE 1

REVENUE PROCESS AUDIT BY CROWE MACKAY



Date: April 12, 2019
To: T. Bob Shahi, Director, Internal Audit Bureau, Government of the Northwest Territories
From: Edward Olson, Practice Leader, Advisory Services, Crowe MacKay LLP
Re: Revenue Audit – GNWT Generated Revenues

SCOPE AND OBJECTIVES

In response to the Internal Audit Bureau (IAB) request for proposal, reference number: 0000002825, for an operational audit reviewing the Revenue Process to determine the control framework and related policies and processes relating to GNWT generated revenue, Crowe MacKay LLP (Crowe) covered the following objectives

- **Objective 1:** Ensure payments received by GNWT and held in temporary suspense accounts are identified and cleared in a timely manner. Determine the main reasons contributing to the need for the use of suspense accounts, and make recommendations for change.
- **Objective 2:** Assess whether there are excess credit balances on customer accounts. The total outstanding credit amounts are currently over \$9,000,000, suggesting this is an area that requires further investigation. Determine the main reasons for credit balances and suggest changes which may reduce the occurrence of these balances or explain the reason for their existence.
- **Objective 3:** Assess methods used to monitor revenue against budget. Ensure active monitoring is in place to timely assess whether revenue expected agrees with revenue actually received. This will include whether procedures are in place to follow-up on revenue not received.
- **Objective 4:** Assess whether there is clarity of roles between Financial and Employee Shared Services (FESS) and the departments for responsibilities in budgeting, monitoring, and reconciling revenues. This will include appropriateness of communication between FESS and the departments to mitigate confusion of responsibilities.
- **Objective 5:** Determine whether revenue rates (i.e. licenses, taxes and other fees) are regularly reviewed and updated by departments. This will also include a review of how potential new revenues are identified whenever possible, the process followed to address these new revenue streams, and whether the new revenue streams are actively pursued.
- **Objective 6:** Maintain the independence of the IAB in all aspects of the scope of this audit engagement.

Focus for this audit remained on evaluating internal controls designed and implemented regarding GNWT generated revenue and in alignment with the Financial Administration Act (FAA) and the Financial Administration Manual (FAM). Crowe reviewed the controls in place at FESS, and within 4 departments chosen for sample testing (Justice; Education, Culture and Employment; Environment and Natural Resources; and Infrastructure). Four department-specific audit reports were issued to address internal control issues.

The scope excluded the NWT Housing Corporation, the GNWT departments other than the 4 noted above, and the 9 public agencies. Audit procedures did not include transaction level revenue testing for this audit.

This audit report relates directly to the objectives noted above and on high-level policies, procedures, control frameworks, and control processes.

Crowe conducted initial meetings with both the IAB as well as with representatives from FESS to identify the current state of activities and areas of concern in GNWT generated revenue processes. This information gathering was conducted as part of the planning process and prior to fieldwork. Feedback received was utilized in assessing risk within revenue processes as well as to suitably plan audit procedures within the scope of this engagement. Some of the key risks identified were:

- Cheques received may not clearly denote the department to which the payment applies. As a result, these funds are placed in a suspense account prior to being reconciled and cleared. Reconciliation and actioning of suspense accounts is not always timely. A number of factors may contribute including, but not limited to, lack of clarity on original invoicing by a department to guide ultimate payment, lack of reference information on individual cheques delaying entry to respective department(s), including inadequate monitoring of revenue by departments to reconcile invoices through to payment receipt. Reconciliations for suspense accounts should be undertaken routinely yet it is not clear whether completion is timely or at all.
- Numerous customer accounts exist with credit balances. An informal evaluation conducted in December 2018 (data run on January 7, 2019) identified 807 customer accounts with credit balances amounting to \$9,260,649.95. This large balance suggests there may be issues with incorrect invoicing, coding, and/or tracking of revenues.
- It is not clear whether departments, including FESS, have a clear understanding and assignment of accountability for identifying those responsible for specific key controls within the full revenue process. Updates to procedures are posted to internal networks and are included in training manuals/courses. However, the risk exists that these updated procedures are not adequately communicated to employees or that employees do not routinely assess changes made to policies and/or procedures in a timely manner. Exposure may also exist with longer tenured employees conducting peer-to-peer training based on their experience and knowledge as compared with referring to most recent policies and procedures for fundamental guidance.
- It is unclear whether departments are adequately monitoring revenue streams and/or conducting reconciliations of revenue received to budget for the fiscal period. Guidance is more complete with respect to procurement activities as compared to revenue processes within the FAA and FAM which drives a high level of attention to procurement policies, procedures and controls.
- Suitability and timeliness of revenue rate reviews is unclear in each department. An understanding of how this activity is prioritized and actioned should be obtained to validate the reasonableness of revenue generated.
- It is unclear whether departments are actively reviewing opportunities for additional sources of revenue. Understanding should be obtained as to how these revenue sources are identified and then tracked for completeness and accuracy of ultimate collection. It was noted that, in some cases, briefing notes are provided departmentally regarding potential new sources of revenue. These are provided in concert with requests for additional funding. Validation and verification is unclear as to whether the additional governmental investment translated into the identified revenue sources by the respective department.
- General tracking and monitoring of revenue-related data may not be performed, may be performed inconsistently, and/or may be performed inefficiently.

Fieldwork was undertaken utilizing the International Standards for the Professional Practice of Internal Auditing as defined by the Institute of Internal Auditors. This ensured a risk-based internal audit plan which applied a methodology that links internal audit procedures to an organization's overall risk management framework.

BACKGROUND

The GNWT has 11 departments and 9 public agencies delivering a range of province-like programs and services to citizens of the Northwest Territories (NWT). Approximately 70% of the revenue to operate the GNWT is from the Government of Canada (GC) grants and transfer payments. The remaining 30% is from taxation, non-renewable resources and general revenues.

The GNWT FAA and the FAM direct how revenues should be processed. Internal financial systems and processes have gone through significant changes. In 2012, the department centric financial processing was phased into a shared service model and was fully operational through the GNWT in 2015. In 2016, the updated FAA was enacted. Most recently, in 2018, the financial information system was upgraded and the financial process has been converted to an electronic approval process.

The 2016-2017 Public Accounts reported \$1.87B in revenue. The 2018-2019 Main Estimate total of \$1.75B in revenue includes Government of Canada grants of 1,256,289,000, transfer payments of \$148,217,000 and \$344,805 in GNWT generated revenue as detailed below:

Revenue Type	Revenue Sub-Type	2018-2019 Main Estimates (\$000's)
Taxation Revenue	Personal Income Tax	103,076
	Corporate Income Tax	31,266
	Tobacco Tax	16,087
	Fuel Tax	24,684
	Payroll Tax	44,866
	Property Taxes and School Levies	29,235
	Insurance Premium Taxes	4,850
		\$251,097
Non-Renewable Resource Revenue	Licenses, Rental and Other Fees	2,380
	Minerals, Oil and Gas Royalties	13,460
	Quarry Fees	180
		\$16,020
General Revenues	Revolving Funds Net Revenue	28,410
	Regulatory Revenues	23,206
	Interest	725
	Investment Income	80
	Lease	3,815
	Program	16,945
	Grants in Kind	214
	Service and miscellaneous	1,293
	Recovery of Prior Year's Expenditures	3,000
		\$77,688
Total Revenues		\$344,805

The table above provides a summary of the various sources of revenue as managed by the GNWT. These revenues are managed via interactions between many participants which include, but are not limited to, the individual departments, FESS, and finance (i.e. Collections, Financial Reporting, and the Management Board Secretariat).

Roles and responsibilities of the various GNWT departments audited are outlined in a number of policies/procedures as well as within legislation. For this audit, both the roles and responsibilities within the Shared Services Agreement and the FAM were utilized as guidance for evaluating activities carried out within each department as well as shared service. A high level summary has been provided below to outline the delineation of these specific revenue functions.

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

Management Board Secretariat:	MBS
Financial Management Board:	FMB
Financial Employees Shared Services	FESS
Procurement Shared Services	PSS
System for Accountability and Management	SAM

Shared Services Agreement – Roles & Responsibilities

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

Financial Administration Manual – Roles & Responsibilities

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

	Department	FESS	Financial Reporting / Collections	MBS / FMB	SAM Team	Comptroller General
	management of all A/R		agency			

DEPARTMENTAL OVERVIEW

Four departments were audited using interviews with key stakeholders as well as a review of policies, procedures, and related control frameworks designed and implemented as at the date of the audit fieldwork. An assessment of each department's treatment of, and approach to, GNWT generated revenue was made, as well as an assessment of their current level of maturity in relation to controls over their respective revenue process. Although the review was performed from a risk-based perspective, it was also determined that a basic level of compliance should be met in relation to revenue treatment in order for department level data to be considered complete and accurate.

Overall, although departments had processes in place which were known and followed in relation to revenue processing, there often were not documented procedures to support these processes. For material revenue streams this can result in varied approaches to revenue management, including the potential for incomplete and inaccurate training to be completed through person-to-person training by employees without reference to defined policies and procedures.

The following sections outline departmental assessment at a high level. Specific findings related to departments can be found in the attached departmental reports (Appendices A-D).

Compliance with FAA & FAM

The FAM has been developed in a manner to ensure that provisions of the FAA have been met. An assessment of each department's compliance with the revenue-related sections of the FAM has therefore been conducted to cover both compliance with FAM, and by extension, with FAA. Departmental compliance is outlined in the chart below by FAM area.

Legend:

C	Compliant;
PC	Partially Compliant
NC	Non-Compliant
UV	Unverifiable

Policy Section	ECE	ENR	INF	DOJ
605 RECORDING REVENUE	UV ²	UV ²	C	UV ²
610 ESTABLISHMENT OF FEES	UV ¹	UV ¹	UV ¹	UV ¹
610.01 RATIONALE FOR FEES CHARGED	NC	PC	NC	NC
620 COLLECTION OF RECEIVABLES	UV ³	UV ³	UV ³	C
620.01 COLLECTION OF ACCOUNTS RECEIVABLE	UV ²⁺³	C	C	C

Note: Where compliance was deemed Unverifiable within the department, Crowe has provided explanation as to the reason why which is denoted via numbering in the table above. The numbering is further defined as follows:

¹ Information not documented by department, therefore not verifiable;

² Process not fully documented, therefore not verifiable; and

³ On Account balances have not been fully reconciled therefore AR may not be received on a timely basis (due to lack of reconciliation this is not yet verifiable).

Maturity Level by Area

Based on the audit work performed, an understanding of the current control environment for revenue-related processes for each department was developed. This summary was used to provide maturity ratings for each of the revenue process areas reviewed as part of this audit. The assessed maturity by department, based on the GNWT Internal Control Capacity Model (Appendix E), is illustrated in the table below. Departments have been provided with steps to be taken for them to achieve the minimum maturity level required. However, due to the risk related to incorrect processing and recording of revenue, it is recommended that additional planning be taken by the departments to reach a higher level of maturity as noted in the individual departmental reports.

Legend:

1	Ad Hoc	Unpredictable environment for which controls have not been designed or implemented
2	Repeatable	Controls are present but inadequately documented and largely dependent on manual intervention. There are no formal communications or training programs related to the controls
3	Defined	Controls are in place and documented, and employees have received formal communications about them. Undetected deviations from controls may occur.
4	Managed	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.
5	Optimized	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.

Revenue Process Area	ECE	ENR	INF	DOJ
ROLE DEFINITION AND RESPONSIBILITIES	3	3	3	3
RATE SETTING & REVIEW	1	1	1	2
BUDGET SETTING	2	2	2	2
INVOICING	2	2	3	2
ACCOUNTS RECEIVABLE REVIEW / COLLECTION	1	2	2	2
MONITORING	2	2	3	3

OBSERVATIONS AND RECOMMENDATIONS

Within the processing of revenue, multiple stakeholders are involved within the departments as well as shared services. Our audit procedures have included discussions with FESS, MBS, FR as well as the 4 departments specifically selected for testing. Department specific findings have been split out as noted above and were provided to each department for review and required management response(s). Each department specific report has been attached as appendices to this report.

The findings noted below relate to the areas of FESS, MBS and FR and not to the departments individually.

Observation 1

FESS had not distributed credit statements to customers in recent years

Based on concerns brought up in the planning phase of this audit, Crowe obtained a SAM listing of all credit receivables. It was noted through initial discussions with the FESS team that credit statements had not been sent out to customers in recent years. Per discussion with FESS after this initial discussion, it was noted the FESS would implement a process going forward for sending out the credit statements. As a result of the lack of distribution of statements, there is increased risk that these items may not be correct, therefore it is important the balances be confirmed before this process is implemented.

Risk Profile:

Risk Impact	When statements are not sent out to customers for verification, there is an increased risk of error. Compounding this are aged credit accounts which have not been addressed in a timely manner and may be more difficult to process and/or reconcile.
Risk Responsibility	Executive Director, Financial and Employee Shared Services
Risk Mitigation Support	Executive Director, ISS

Recommendations:

We recommend that:

- Current outstanding credit balances should be fully reviewed for completeness and accuracy as a one-time project.
- Credit statements should be sent to customers after a full review has been completed, and a process be developed for these to be sent (electronically if possible) on a quarterly basis going forward.
- A process should be formalized and documented to ensure timely review of credit balances on a monthly basis.

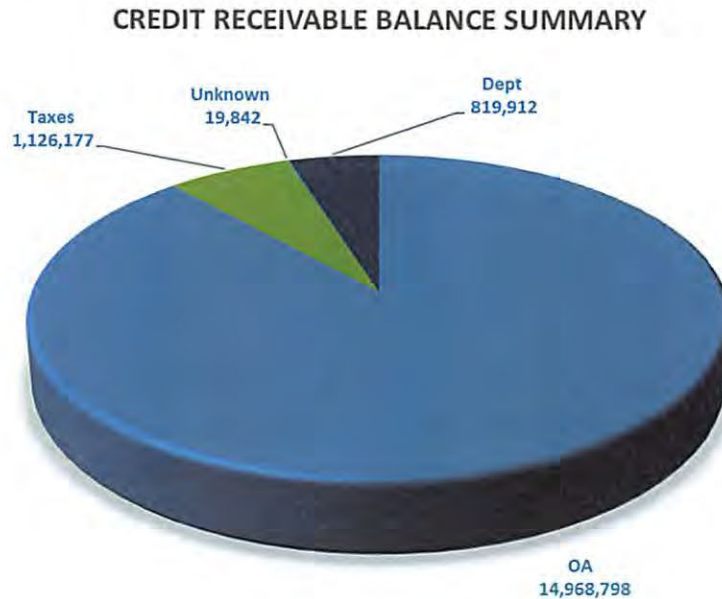
Management Response:

Action Plan:	Completion Date:
a) Reporting, Treasury and Risk Management (RTR) is currently reviewing credit balances in AR over \$10k as part of the 2018/19 year end. RTR has a planned project for this fall to follow up on other credits in AR.	March 31, 2019 December 31, 2019
b) Subsequent to the action plan in a) above, FESS will send statements with credit balances to customers	December 31, 2019
c) RTR will ensure the process be documented to ensure a timely review of credit balances	June 30, 2019

Observation 2

On Account "OA" coding not effectively monitored

Building on Observation 1, related to credit balances, further investigation was undertaken during the audit. A report outlining all credit receivable balances was obtained from the SAM team and analyzed. The results have been outlined in the following chart:



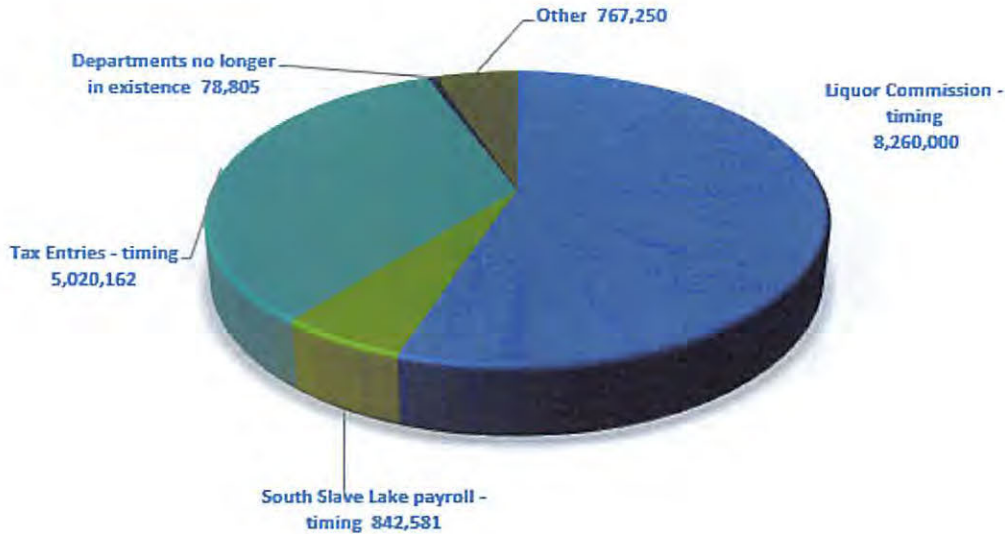
Primary coding for credit balances, and all balances greater than \$100,000 (other than one entry relating to a timing difference for fuel tax), were coded to OA. These entries totaled \$14,968,798. Steps were then taken to determine when the OA coding is used.

When FESS receives cheque payments and it is not apparent which department the payment should be allocated to, FESS will post it to an OA which results in a credit to the customer until the item is resolved (note: customer may owe more than one department). Should the balance be appropriately reconciled to the correct department, the closing entry removes this OA receivable with a credit to the correct department and respective accounts receivable balance. The posting may be made to a department's OA account if the department is identified but not yet confirmed, or it may be coded to the finance department's OA account if the department is not known.

OA coding is also applied when monies are received in advance of the processing of the related invoice or tax return, as applicable.

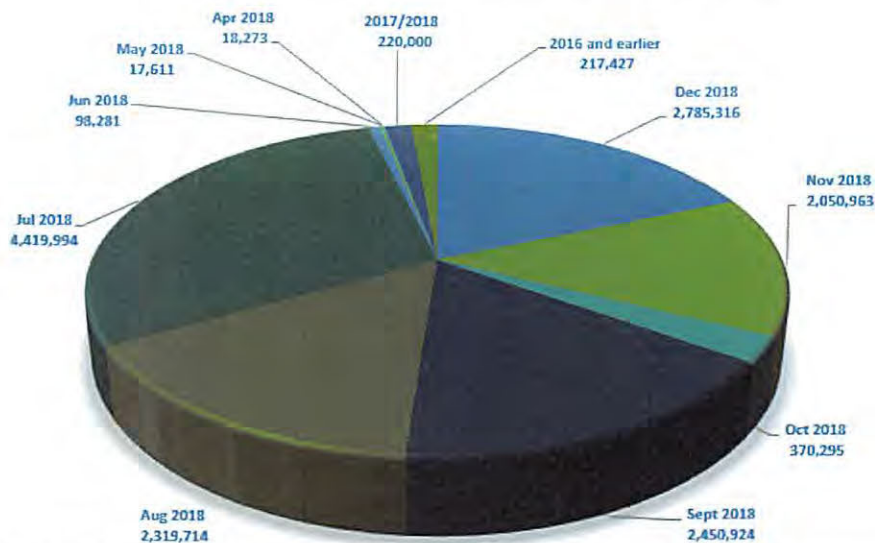
Per a review of all OA credit balances, the breakdown of type of OA is as follows:

"ON ACCOUNT" BREAKDOWN BY ENTRY TYPE



The large bulk of OA entries relate to tax entries where money has been received in advance of the processing of the related tax return. These credit balances are therefore due to timing differences and are not of concern within the scope of this audit. The balance for the South Slave Lake was in relation to payroll and a check of the balance in mid-February showed that it had been cleared. There were two remaining areas of concern. The first related to entries labelled "other" which was made up of multiple smaller entries with varying descriptions. The second related to entries which were for departments no longer in existence. As noted in relation to the EFT transfers, it is important that all balances are clearly identified and allocated as there is a responsibility by the GNWT to its clients to correctly record the money that is collected. An assessment of the age of entries was performed as is shown in the pie chart below:

"ON ACCOUNT" BY YEAR (2018/2019 YEAR TO DEC 2018)



This analysis suggests that although the numbers may be smaller in size there are some long outstanding entries that have not been cleared and GNWT departments have a responsibility to their clients to correctly record revenue. It has therefore been recommended in the observations below that a review of the OA credit balances be performed by FESS on a set periodic basis in order to ensure that these entries have been cleared in a timely manner. This process has been assigned to FESS as it is the centralized service which has access to all of the entries and likely processed the original entry.

Risk Profile:

Risk Impact	Without full monitoring of OA-coded accounts, there is an increased risk that these codes will be misused, or that full identification of cheques received and reconciled to underlying customer accounts is incomplete.
Risk Responsibility	Executive Director, Financial and Employee Shared Services
Risk Mitigation Support	

Recommendations:

We recommend that:

- FESS develop a written process whereby all OA-coded credits are identified monthly from SAM and then reviewed to ensure they are correct and have not been outstanding for long periods of time.
- FESS should communicate all balances outstanding from the review noted in (a) to departments to ensure departmental review is undertaken to complete clearing of all accounts.
- A one-time project should be undertaken to identify the current long outstanding balances which should then be reconciled and cleared.

Management Response:

Action Plan:	Completion Date:
a) FESS is updating business processes and internal guidelines to ensure due diligence when applying payments received.	August 2019
b) FESS will ensure business processes are shared with departments to support departmental review of any credit balances outstanding.	August 2019
c) RTR has project planned for this fall to follow up on other credits in AR	December 31, 2019

Observation 3**A government-wide policy is not established regarding the use of On Account "OA" coding**

Building on Observation 2, related to the use of On Account "OA" coding, further investigation was undertaken during the audit. This coding is used by FESS for payments received which are not reconciled with underlying customer accounts. OA is also used at the department level as well as within Finance. Payment for taxes, where the related return has not yet been reviewed, may either be coded to a tax code, or coded to OA. OA coding seems to be used by both FESS as well as departments yet no written policies or procedures have been established to clarify correct use.

There are old items (back to 2009) with "OA" coding suggesting this coding may have been used incorrectly, or that monitoring of OA items is not adequate.

A GNWT wide policy on how and when OA coding can be used should be prepared to ensure coding is correctly applied. As FESS has access to all accounts and departmental information, it is also recommended that FESS prepare a periodic (monthly or quarterly) statement of all outstanding OA items which should then be sent to all departments for review. This will allow departments to identify items which may have been sent to an incorrect department when the cheque was originally received.

Risk Profile:

Risk Impact	Without written processes in place for the use of the "On Account" coding across the government, there is increased risk of misuse of the coding, and incorrect or missing monitoring of accounts with this designation.
Risk Responsibility	Assistant Comptroller General
Risk Mitigation Support	DFA community

Recommendations:

We recommend that:

- a) A government-wide procedure be established and documented for the correct use of OA coding, including delineation of when this coding can and cannot be utilized.
- b) Training should be implemented to ensure all departments and areas understand and follow this policy.
- c) Monitor and report on the proper usage of OA

Management Response:

Action Plan:	Completion Date:
a) The current procedures will be documented and made available to all parties	August 2019
b) RTR and FESS will ensure training continues to be offered	August 2019 & ongoing
c) Annually monitor and report on the use of OA balance	Starting April 2020

Observation 4

FESS requested more information from departments when data was readily available

Cheques are processed by both departments and FESS. FESS processes the bulk of cheques received. Departments that receive cheques will either forward them to FESS for processing or will process them through their cash drawer (where applicable). In the case of the department receiving cheques, the coding would be known by the department and processing would be clear for matching with respective invoice(s).

When FESS receives a cheque, the process is to review the cheque and associated supporting documents to identify the department and specific invoice to which the cheque will apply. The payment is then posted against the invoice. If the department is known (or thought to be known), yet the specific invoice number is not, the payment is coded to that department's "On Account" (OA) account. A notification is sent to the department's general email alerting of the inability to apply payment to a specific invoice. The department is responsible for replying within 2 days. If the department and invoice are not known, the payment is coded to the finance department's OA. This audit's assessment and investigation into OA's has been discussed in further detail below under the "Credit Balances" section with respective details for outstanding OA account items.

Through discussions with the departments during this audit, it was noted that there are times when on occasion FESS sends cheques through to a department for additional information when the respective information is clearly discernible that denotes where payment is to be applied (i.e. invoice number) or that the payment is applicable to a different department. Crowe obtained emails outlining examples of this issue from three of the four departments selected for testing, with clear documentation for 3 different incidents noted. A review of the FESS procedures revealed that although their general processes are documented, there is no specific set of instructions which outline how a cheque review should be performed. A checklist to guide FESS staff would fulfill this need and has been recommended below.

Risk Profile:

Risk Impact	Without clear procedures in place there is increased risk that FESS personnel will forward items to the departments incorrectly, resulting in additional work for departments to confirm payments that are not theirs.
Risk Responsibility	Executive Director, Financial and Employee Shared Services
Risk Mitigation Support	

Recommendations:

We recommend that:

- a) A checklist of items be created and communicated to front line staff that identifies those steps to be taken by FESS to ensure correct action is taken before departments are contacted.
- b) Monitor and track the proper use of checklist.

Management Response:

Action Plan:	Completion Date:
a) As outlined in Observation 2, FESS will be updating guidelines to ensure correct steps are taken.	August 2019
b) FESS will ensure guidelines include process of monitoring of payment application	August 2019

Observation 5

Per discussion with FESS, the departments, SAM, MBS and various areas of Finance related to revenue reporting and recording, there is no set training program for those involved in revenue activities which are mandatory for completion.

Training in revenue-related procedures is not a requirement for specific job titles or roles. There are two revenue-specific training courses within the SAM system relating to billing and cash drawer processes. Review of training records revealed that GNWT staff are completing these courses each year. In 2017, 100 individuals completed the Cash Drawer course and 157 completed the Billing course. In 2018, 86 people completed the Cash Drawer course and 159 people completed the billing course. These courses only address very particular aspects of revenue related to the SAM system, rather than the larger concern of understanding revenue concepts and risks.

Discussion with department and FESS representatives revealed there to be varying levels of understanding of revenue concepts depending on the background of the individual employee. This, and the movement of staff throughout the government over their careers including turnover, increases the risk that an incomplete training program will result in staff who do not fully understand their duties and the impact of their daily responsibilities on their respective department including the GNWT overall.

Role changes and turnover within the government results in an ever-moving and developing work force. For those entering new roles, training may be incomplete or inconsistently provided. There does not appear to be training required for certain roles at this time.

Risk Profile:

Risk Impact	Without required training in complex financial areas such as revenue, those in oversight roles may not understand the risks involved when their staff carry out procedures incorrectly, or when processes are undocumented or inaccurate.
-------------	---

Risk Responsibility	Comptroller General
Risk Mitigation Support	Assistant Comptroller General Executive Directors – FESS & ISS Director MBS DFA community

Recommendations:

We recommend that:

- A training program for complex financial areas such as revenue be implemented which is required for management roles, or those with oversight in financial areas.
- Where such programs already exist, but does not take into account revenue processes, it is recommended that it be included in future development.
- Training should also include clarification of the roles performed by FESS, PSS and Departments to ensure these are clearly understood.
- Pre and post testing be done to track the effectiveness of training

Management Response:

Action Plan:	Completion Date:
a) RTR already has a mandate to create training modules which will include Revenue training.	October 2019
b) The first step is to develop a framework to prioritize all training needs for users.	October 2019
c) General process will be included in training but it must be generic for other users.	October 2019
d) Feedback on training will be sought.	After October 2019

Observation 6

FR has implemented a semi-regular report which is sent to departments with a list of unclaimed payments received as EFT payments.

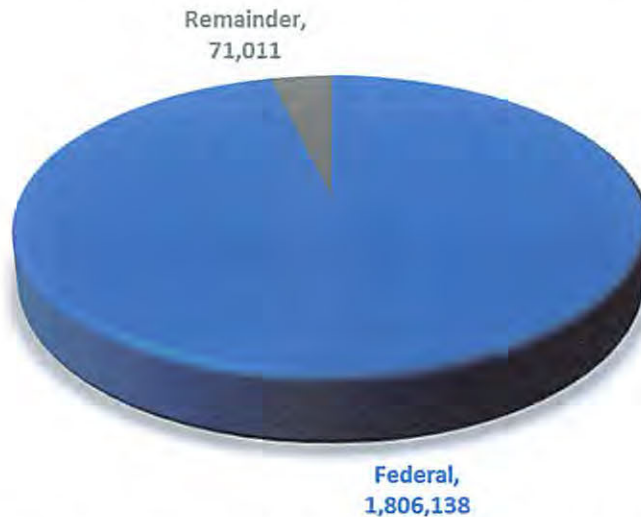
When electronic fund transfers (EFT) are processed, they are received into the Consolidated Revenue account. The Financial Reporting (FR) group within Finance is responsible for reviewing these items. If they have been provided the payment notification initially by a department, FR will validate the money has been received and will then forward the data to FESS for posting. If they have not received a payment notification from the department in advance, and the deposit has been entered into the bank, they then undertake further investigation to determine which department the deposit belongs. If they are able to determine where the deposit belongs, they then forward the information to the department with a request for appropriate coding, including the respective invoice number. Once this information is received, FR will then send the data to FESS for posting.

If FR staff cannot determine which department the deposit belongs, it is then added to the "Unclaimed Deposit List" which is then emailed out to each department finance manager for review. This review is intended to solicit feedback on where the deposit should be allocated. Historically, this list was not sent out in a timely manner but was released to the departments annually. Changes have been made to this process to ensure the departments receive information on a more routine basis.

Should no response be received from the departments, and the balance remains on the Unclaimed Deposit List at year end, the money is claimed by finance for general revenues. It is at this point the departments can no longer claim the revenue. Departments have noted that they appreciate the timelier receipt of communication relating to the unclaimed deposits as compared to only receiving at year end. It has been recommended that this be made a monthly report that goes out on a particular day to formalize the process.

A review was performed of the total balance outstanding which was not claimed for the 2017/2018 fiscal year end. Please refer to the pie chart below for details.

2017/2018 UNRECONCILED EFTS



The bulk of the outstanding items (96%) were two federal payments of \$1,352,539 and \$453,174 which resulted from a department not identifying the payment until after the year end had passed.

The remaining \$71,011 was comprised of numerous balances. It is therefore likely that these items were not noted by departments in their revenue reviews due to the small nature of the payments. It is important to note that although the items may seem small, they may not be considered small payments to those making them, and it is important they are identified correctly. Ongoing timely reporting from FR to the departments has begun this year and will assist in ensuring the majority of payments are reconciled in a timely manner when they are most likely to be recognized. This report is appreciated by departments yet is not sent out on a routine, scheduled basis. Response times are also not set for the departments so that unreconciled items can be timely reviewed and cleared.

Risk Profile:

Risk Impact	Without a response timeline, the departments may not feel that they must deal with the report in a timely manner, this can increase the risk that an unclaimed balance will remain outstanding at year end and be taken into general revenues. A set reporting timeframe also increases the likelihood of timely responses.
Risk Responsibility	Manager, Financial Reporting & Collections
Risk Mitigation Support	

Recommendations:

We recommend that:

- The report be sent out on set monthly basis to ensure departments are aware of the expectation to address and action outstanding items.
- Establish a required response period where departments are to review and provide feedback to FR regarding any unclaimed balances which are theirs.

Management Response:

Action Plan:	Completion Date:
a) This report is already sent out more frequently including ad-hoc requests and end of year immediate follow-up	Ongoing
b) Departments are requested to respond with dates when appropriate	Ongoing

Observation 7

FR has processes which are followed in relation to EFT notifications, but these are not currently documented.

Building on Observation 6, regarding FR's treatment of EFT's, further investigation was undertaken during the audit. FR has extensive processes which are followed in relation to EFT notifications. Although staff were clearly able to explain what they do during the interview process, the steps for these processes are not formally documented to provide them with consistency for operational application as well as to provide guidance for training of new staff members.

Risk Profile:

Risk Impact	Without documented procedures, there is increased risk that different employees will carry out processes incorrectly, and that new employees will have more difficulty performing their duties.
Risk Responsibility	Manager, Financial Reporting & Collections
Risk Mitigation Support	

Recommendations:

We recommend that:

- a) Procedures related to processing of EFT transactions be fully documented.

Management Response:

Action Plan:	Completion Date:
a) ETF procedures will be documented	August 2019

Observation 8

MBS documentation relating to variance review is not in place

Departments and the MBS play the largest roles in terms of monitoring revenues. Departments prepare monthly variance reports and submit to MBS. From these reports MBS staff prepare quarterly reporting for release to the FMB. MBS staff follow up with the departments in relation to any variances that are unexpected and where explanations are insufficient. Examples of email correspondence relating to variance explanations were reviewed during the audit to confirm that MBS staff are asking suitable questions about variances when explanations are not clear. Although MBS staff appear to be comfortable with their monitoring role, there are currently no documented processes which outline how the analysis of variance reports are carried out. It has been recommended that these be prepared.

Variance reporting for each of the departments selected for testing was reviewed for the period from April 1, 2018 to September 30, 2018 as part of the audit work performed. Clear commentary was in place for each variance noted.

Risk Profile:

Risk Impact	Lack of documentation can lead to inconsistent application of control activities, which can result in increased risk of error. In this particular case, the risk that inadequate variance explanations are not noted and corrected may be increased.
Risk Responsibility	Director, Management Board Secretariat
Risk Mitigation Support	

Recommendations:

We recommend that:

- a) MBS develop a complete set of written policies and procedures outlining the activities of the MBS revenue-related activities.
- b) Once developed, ensure those employees involved in critical revenue receive training in line with the policy.

Management Response:

Action Plan:	Completion Date:
a) MBS will update the existing variance reporting section in the FMB handbook.	August 2019
b) Training will be provided as required	August 2019

MANAGEMENT INFORMATION FOR DISCUSSION

During the audit, Crowe made a number of observations for management consideration. The observations below outline processes observed in areas covered by the objectives of this audit. We are not making any specific recommendations on these observations.

Observation 1

FESS has documentation in place which defines those specific areas of processing for which they are responsible to assist their employees in understanding what must be done including what is expected of individual departments. This includes what is to be provided to and/or obtained from departments throughout the revenue cycle.

Departments have differing levels of role clarity and documentation, from not documented through to partial documentation. Department level roles and responsibilities are discussed in the department reports individually for what was identified during this audit.

Considering the roles and responsibilities which have been delineated within shared services as well as the departments, Crowe also analyzed the interaction(s) between each to assess effectiveness and efficiency of operations. Understanding that the responsibility for completeness and accuracy of the revenue process is shared, there are also certain activities within the full revenue cycle which are specifically assigned to either FESS or the departments. While roles are specifically defined, this relationship between FESS and the departments was the largest cause for confusion which was identified throughout this audit. Lack of clarity regarding the processing of cheques was commonly heard as a cause for this frustration and confusion. It is uncertain as to whether the multiple touchpoints relating to this process between FESS and the departments was the cause of the confusion or the lack of training on who was ultimately responsible and for what. Both of these issues have been dealt with in observations 5 and 8 noted above, and addressing those areas should assist in making this interaction more successful.

Observation 2

Rate setting and review is the role of each department. FESS, MBS and SAM are not involved in these rate processes for revenue generation. Generally, rates are established to provide cost recovery for related products and services, if not in full then in part. The expectation of each department is that

legislation identifying rates is to be reviewed on a routine basis. Where new revenue sources are identified, these are to be reviewed as they arise. Rate setting and review activities within each department selected for testing within this audit have been specifically addressed in their respective reports.

Observation 3

Budgeting for revenue sources is undertaken by each department annually. Departments are responsible for providing budgets and underlying assumptions to MBS along with explanations for any changes from prior revenue streams. Reporting must be undertaken via a pre-established template which is laid out in the "2019-2020 Main Estimates Instructions" document.

Estimates must include explanations for new revenue including variances from prior years. MBS staff then conduct a review of estimates and associated commentary to validate positions taken and evidence to support budget assumptions. After this review, should any unexpected changes and/or unusual items arise where explanations are not sufficient, MBS staff will contact the department to obtain a better understanding of the estimate. The budgets are then approved by the FMB.

MBS staff interviewed as part of this audit clearly understand their role and responsibilities. This has been assessed through review of communications with departments (i.e. email communications) and related questions asked regarding budget variances. MBS has also established a formalized reporting schedule for items due from the departments including tracking of when information is actually received, including what is outstanding. This assists with their roles in ensuring all aspects from budgeting through explanation of variances from budget.

Observation 4

Invoicing is initiated by each department, accounting approval is provided by FESS, with final invoices released by the department. There are circumstances where invoices are not required. This applies to departments where revenue sources such as licensing require payment to be provided onsite as the service is provided in return for payment on site. A receipt would be issued at the time of payment, but invoices are not used for items of this nature. Each department has varying levels of invoice use depending on their type of revenue source(s).

Once an invoice has been recorded, the accounts receivable will remain until the payment is applied. As noted under the Payment Processing section, there may be some items placed "On Account" which are never applied to a specific invoice. The A/R related to those invoices should therefore remain outstanding and be noted during routine A/R review to ensure necessary follow-up is completed (addressed under Section D, Observation 3 above).

Invoicing has been discussed in each of the department reports, along with any specific issues and recommendations.

Observation 5

Departments are responsible for customer accounts and ultimate payment received. However, when accounts exceed 90 days outstanding, they automatically transfer from the department to Collections. Throughout fieldwork, this 90 day transfer was clearly understood by all parties. The Collections team assumes responsibility for collection actions, including external collection agency use, up to legal proceedings when necessary.

The FAM requires that any items over 30 days have a written notice be provided to the customer. This process related to A/R management is handled by FESS which sends out debit statements on the 10th of each month to applicable customers. Going forward, credit statements will also be sent out the customers on a set periodic basis.

The A/R process and any related issues to be addressed by management have been addressed in each of the department reports individually.

APPENDIX A

DEPARTMENT OF EDUCATION, CULTURE, AND EMPLOYMENT

DEPARTMENT OF EDUCATION, CULTURE, AND EMPLOYMENT

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 Education, Culture and Employment (ECE) meets its responsibilities through the following functions:

- Corporate Management;
- Culture, Heritage and Languages;
- Early Childhood and School Services;
- Labour Development and Standards and,
- Income Security.

General revenues generated by ECE consist of the following:

- Regulatory Revenues – Teacher Certification Fees, Apprenticeship Fees and Other Fees;
- Interest - Student Loan Fund interest;
- Lease – Museum Café (rent);
- Program Revenues – Care and Storage of Government of Nunavut Museum and Archive Collection and Program Recipient Recoveries and,
- Service and Miscellaneous revenue.

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

- Teacher Certification Fees, Apprenticeship Fees and Other Fees are the responsibility of Education Operations and Development and Financial Operations;
- Student loan fund interest is the responsibility of the Manager and Senior Finance Officer of Divisional Financial Services;
- Lease revenues are the responsibility of Culture and Heritage;
- Care and Storage of Government of Nunavut Museum and Archive Collection revenues are the responsibility of Culture and Heritage.

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

ECE 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, Finance and Capital Planning, 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 ECE department to provide the evidence necessary to conclude on internal control effectiveness, Crowe has concluded that additional work is required by ECE 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
605 – Recording Revenue		
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.	Unverifiable	Unable to verify if revenue earned is recorded in accordance with approved systems and procedures because not all significant approved systems and procedures

Section Policy	Compliance Assessment	Reason for Non-Compliance
		are documented.
610 – Establishment of Fees		
<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>	Unverifiable	<p>Regulated rates are reviewed every five years as per FMB direction.</p> <p>The rationale for rate changes or unchanged rates at the five year review for other than inflationary changes are not documented, as such it is not verifiable whether the rates address current costs of the related services or license.</p>
<p>IB610.01 Rationale for Fees Charged</p> <p>GNWT Departments and Public Agencies are to ensure that fees are collected, safeguarded, and accounted for.</p> <p>A rationale for each fee charged must be kept available for audit purposes.</p> <p>The rationale in support of each fee charged must include:</p> <ul style="list-style-type: none"> - pricing details; - the price/rate basis, including direct, indirect, and accounting and system costs and, - the time period for cyclical fee reviews. <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>	Non-Compliant	<p>The rationale for rate changes or unchanged rates other than inflationary changes at the five year review are not documented.</p>
620 – Collection of Receivables		
<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>	Unverifiable	<p>Although the department has been rated compliant with the specifics of section IB 620.01 below, the overall 620 compliance cannot be verified due to the potential issues noted with the credit receivables with "On Account" coding.</p> <p><i>See Observation 9 below.</i></p>

Section Policy	Compliance Assessment	Reason for Non-Compliance
<p>IB 620.01 Collection of Accounts Receivable</p> <p>Except as described below, an invoice must be prepared, recorded, and delivered to the debtor as soon as a receivable is created and the debtor must be given 30 calendar days from the date of the invoice to return payment to the GNWT or Public Agency.</p> <p>If payment is not received within 30 days of the date of the invoice, the responsible department or Public Agency shall attempt to collect by notifying the debtor in writing that payment is overdue and payable immediately. At this point, the debt has become an overdue receivable.</p> <p>If payment is not received during the next 30 days (i.e., within 60 days of the date of the invoice) the responsible department or Public Agency shall attempt to collect again by notifying the debtor by telephone and in writing that payment is now 30 days overdue and payable immediately.</p> <p>If payment is not received during the next 30 days (i.e., within 90 days of the date of the invoice) the overdue receivable becomes a delinquent account receivable. The responsible department or Public Agency shall:</p> <p>attempt to collect again by notifying the debtor that payment is now 60 days overdue and payable immediately; and transfer collection responsibility to the Financial Reporting and Collections Section, Finance, immediately.</p>	<p>Unverifiable</p>	<p>All revenues with the exception of student loan interest are received when earned. For student loan interest, fees are calculated monthly and added to the students' accounts.</p> <p>The department sends letters for student loan payments outstanding more than 30-90 days, per the department's processes.</p> <p>The collection responsibility is assigned correctly to the collections department at 90 days.</p>

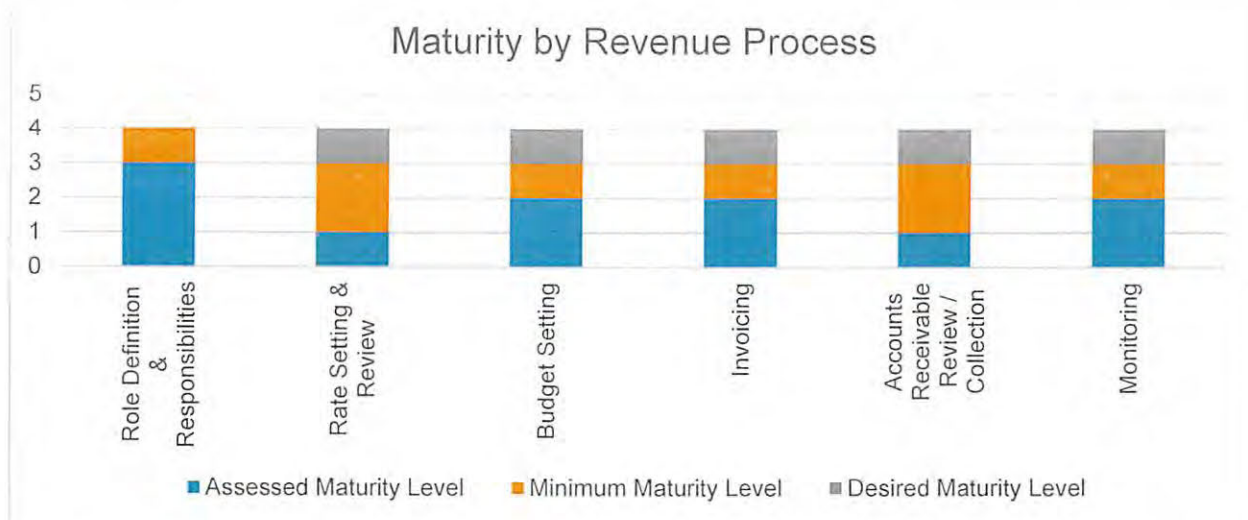
Maturity Rating Considering GNWT Internal Control Capacity Model

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
Role Definition and Responsibilities 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"> Job descriptions exist for the positions outlined above under departmental background as responsible for the department's general revenue functions. Job descriptions include responsibilities related to specific general revenue cycle components. Job descriptions reviewed by Crowe have been updated within the last four years.
Rate Setting & Review 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"> Majority of rates and fees are regulated and are charged in accordance with regulations. Regulated rates and fees are reviewed every five years per FMB direction. Rationale for fees is not documented. Non-regulated rates and fees are not reviewed on a set periodic basis and policies and processes are not documented. New sources of revenue are considered when new programs or initiatives are planned but a formal process does not exist. <p><i>See Observation 1, 2 and 3.</i></p>
Budget Setting The department clearly defines and documents the revenues expected for each year with explanations for any	Repeatable	<ul style="list-style-type: none"> Clarity on roles and responsibilities exists for ECE Financial and Capital Planning. ECE Financial and Capital planning prepares the operating budget and revenue estimates. Budget of significant revenues is based on student

Revenue Process Area	Assessed Maturity Level	Findings and Comments
material changes from prior years.		loan portfolios, leases, expectations, interest rates and revenues are extrapolated accordingly. Insignificant revenues are based on prior year actuals and estimates. <ul style="list-style-type: none"> Assumptions and rationale for estimates are not documented. See Observation 4.
Invoicing The department ensures that invoices are prepared in a timely manner, and are accurate and complete.	Repeatable	<ul style="list-style-type: none"> Invoices are not issued for the department's revenue streams because payment is received at the time of service, with the exception of student loan fund interest, for which statements are provided, and lease revenues, which are received in accordance with the lease terms. Processes are in place to record revenues received in cash, cheque, credit card or by online payment at the time the service is provided. Processes are in place to ensure all revenues earned are recorded as revenues for revenues received by cheque or direct payment. Processes are documented for student loan fund interest but are not documented for all significant revenue streams. See Observation 5.
Accounts Receivable Review / Collection The department monitors receivables on a set periodic basis and ensures that follow-up takes place if revenues are not received as expected.	Ad Hoc	<ul style="list-style-type: none"> The department has a "Finance General" email established for emails from FESS and a department representative has been assigned. The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque. The number of receipts by cheque by the department are insignificant, the majority are received by direct payment. The department's process for addressing emails received from FESS is not documented. 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. The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting. The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting. The procedures to be taken when an unclaimed

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<p>deposits email is received from Department of Finance - Financial Reporting have not been established and documented.</p> <ul style="list-style-type: none"> Accounts receivable were not reviewed until recently. Accounts receivable balance at December 31, 2018 was \$(42,857.67) which has been outstanding more than 120 days. "On Account" balances in the department's accounts receivable were not reviewed until recently. "On Account" balances at December 30, 2018 amounted to \$(17,841.48). The department understands the role and responsibility of the Collections unit. <p><i>See Observations 6, 7, 8 and 9.</i></p>
<p>Monitoring</p> <p>The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are not being received as expected.</p>	<p>Repeatable</p>	<ul style="list-style-type: none"> Monthly and quarterly variances are prepared by Financial Operations based on budgeted revenues versus actuals revenues per reports from SAM. Explanations for variances are documented. Variance reports are reviewed and provided to Management Board Secretariat. Process for variance analysis is not documented. <p><i>See Observations 10.</i></p>

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 processes is lacking.
- The department informally reviews non-regulated rates and fees, but a policy and process has not been designed and documented for the review of all rates and fees.

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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

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

- b) For regulated rates, documentation should be made to support that rates are reasonable to cover off the current costs associated with the services for which fees are being charged or the rationale for rate changes.

Management Response:

Action Plan	Completion Date:
a) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019
b) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019

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 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- a) 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:
a) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

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) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019

Observation 4

Procedures for review of budgeted revenues assumptions and rationale is not fully documented.

- Significant general revenue budgets are based on statistical information, assumptions, and rationales, but the process to develop the revenue budget and document the rationale is not documented.

Risk Profile:

Risk Impact	A lack of documentation of process and procedures to develop the revenues budgets using various applicable metrics can create inconsistencies in budgeted revenues year over year, especially if staff turnover occurs.
Risk Responsibility	Director, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- a) Process and procedures be documented related to the development of revenue budgets, including the inputs and assumptions required.

Management Response:

Action Plan	Completion Date:
a) Partially documented, will review the documentation and add where needed.	September 30, 2019

Observation 5

Revenue processes are not fully documented.

- Processes are in place for each significant revenue stream to ensure revenues earned are recorded but are only documented for student loan fund interest revenues; processes are not documented for other significant revenues.

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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- 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) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 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, Financial Operations, 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 ECE 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019
b) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 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 ECE revenues will be unrecorded.
Risk Responsibility	Director, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

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) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 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, Financial Operations, 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 to the applicable department staff for review.
- If a payment is identified by department staff as being for ECE and the purpose of the receipt is known the department staff will email the Manager, Financial Operations with the coding.
- The Manager, Financial Operations 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019
b) Management agrees with the	September 30, 2019

recommendation and will create and document the policy/procedures as requested.	
---	--

Observation 9

Processes have not been designed and documented to review accounts receivable and “On Account” accounts receivable.

- Accounts receivable are not being reviewed on a regular basis, although there have been recent discussions to start this process.
- 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, ECE’s accounts receivable included \$17,841 of “On Account” credit balances from 2014/15 fiscal year to 2018/19 fiscal year, broken down as follows:
 - 2014/15 fiscal \$1,049
 - 2015/16 fiscal \$155
 - 2016/17 fiscal \$2,882
 - 2017/18 fiscal \$3,329
 - 2018/19 fiscal \$10,426
- “On Account” accounts receivable are not being reviewed on a regular basis.

Risk Profile:

Risk Impact	Without a process being designed and documented, “On Account” receivables are not 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- a) A formal process should be designed and documented that ensures accounts receivable are reviewed monthly.
- b) The process should ensure the “On Account” receivables are included in the monthly review and that explanations are provided for any outstanding balances existing for more than 30 days.

Management Response:

Action Plan	Completion Date:
a) Management has started reviewing as of December 2018.	September 30, 2019
b) Going forward, this review will include OA receivables and explanations will be provided for outstanding balances existing for more than 30 days.	September 30, 2019

Observation 10

Variance analysis preparation process has not been documented.

- Variance analysis is performed monthly and quarterly based on reporting from SAM, with variance explanations provided and sent to MBS. 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, Education, Culture and Employment, Finance and Capital Planning
Risk Mitigation Support	Manager, Financial Operations

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) Management agrees with the recommendation and will create and document the policy/procedures as requested.	September 30, 2019

APPENDIX B

DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES

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
605 – Recording Revenue		
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.	Unverifiable	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
610 – Establishment of Fees		
<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>	Unverifiable	<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>IB610.01 Rationale for Fees Charged</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"> - pricing details; - the price/rate basis, including direct, indirect, and accounting and system costs; and, - the time period for cyclical fee reviews. <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>	Partially Compliant	<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>
620 – Collection of Receivables		
<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>	Unverifiable	<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>IB 620.01 Collection of Accounts Receivable</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>	Compliant	<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: 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>

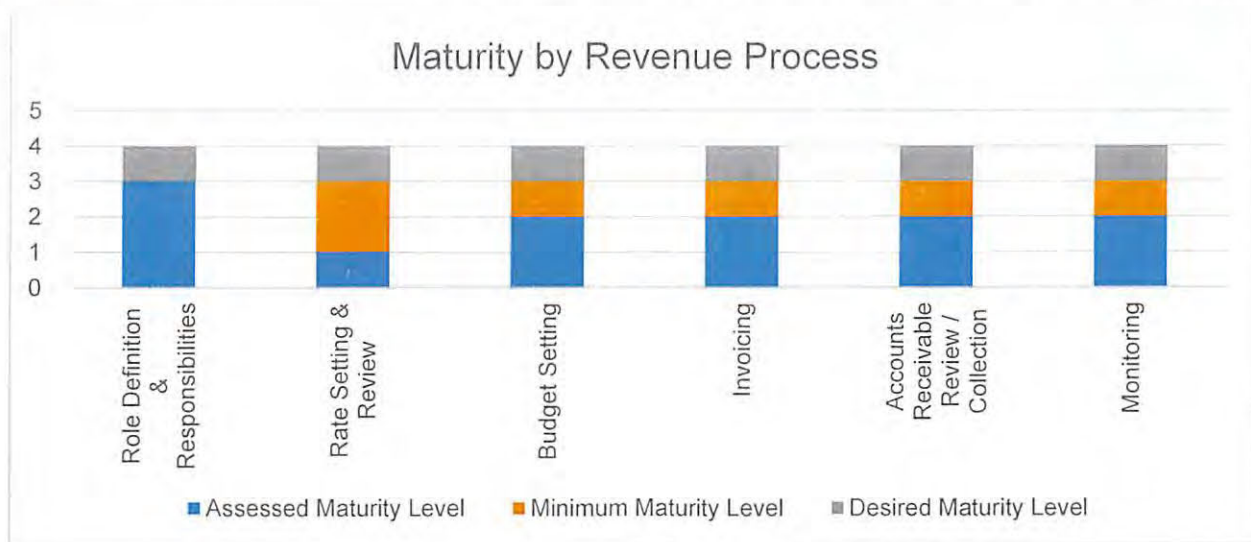
Maturity Rating Considering GNWT Internal Control Capacity Model

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

Revenue Process Area	Assessed Maturity Level	Findings and Comments
material changes from prior years.		<ul style="list-style-type: none"> Budget of revenues is based on prior year estimates and actuals with input from program managers not on statistical information. Assumptions and rationale for estimates are not documented. <p><i>See Observation 4.</i></p>
<p>Invoicing</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"> 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. Processes are in place to record revenues received in cash or by online payment at the time the service is provided. Processes are in place to ensure all revenues earned are recorded as revenues for revenues received by cheque or direct payment. Processes are not fully documented for each revenue stream. <p><i>See Observation 5.</i></p>
<p>Accounts Receivable Review / Collection</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"> The department has a "Finance General" email established for emails from FESS and a department representative has been assigned. The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque. The department's process for addressing emails received from FESS is not documented. 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. The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting. The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting. The procedures to be taken when an unclaimed deposits email is received from Department of Finance - Financial Reporting have not been established and documented. 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

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<p>days.</p> <ul style="list-style-type: none"> “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. The department understands the role and responsibility of the Collections unit. <p>See Observations 6, 7, 8 and 9.</p>
<p>Monitoring</p> <p>The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are not being received as expected.</p>	Repeatable	<ul style="list-style-type: none"> Monthly and quarterly variances are prepared by Financial Planning based on budgeted revenues versus actuals revenues per reports from SAM. Explanations for variances are documented. Variance reports are reviewed and provided to Management Board Secretariat. Process for variance analysis is not documented. <p>See Observation 10.</p>

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:
<p>a) ENR is in the process of designing 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>	June 30, 2019

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:
<p>a) ENR is in the process of documenting the process involved in setting & reviewing the rates.</p> <p>Staff members responsible for each revenue stream will document the rationale for the rate as it was explained to the auditors</p>	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:

- 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:

- a) 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.
- b) Processes and procedures should be documented to address unclaimed deposit emails from Financial Reporting.

Management Response:

Action Plan	Completion Date:
<p>a) ENR is in the process of designing and documenting procedures of identifying unclaimed deposits provided to the department by Financial Reporting.</p> <p>The new procedures will be shared with all concerned staff members and also stored in DIIMS.</p>	May 31, 2019
<p>b) ENR is in the process of designing and documenting procedures of handling the emails received from Financial Reporting in relation to unclaimed deposits.</p> <p>The new procedures will be shared with all concerned staff members and also stored in DIIMS.</p>	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 formal process should be documented that ensures “On Account” receivables are reviewed monthly
- 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

APPENDIX C

DEPARTMENT OF INFRASTRUCTURE

DEPARTMENT OF INFRASTRUCTURE

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 Infrastructure (INF) meets its responsibilities through the following functions:

- Corporate Management;
- Asset Management;
- Programs and Services, and;
- Regional Operations.

General revenues generated by INF consist of the following:

- Revolving Funds Net Revenue – Marine Transportation Services Revolving Fund, Yellowknife Airport Revolving Fund and Petroleum Products Revolving Fund;
- Lease Revenue – Airports lease and rental revenue, rentals to others;
- Program Revenues – Canadian Air Transport Security Authorization Agreement, Nav Canada Occupancy Agreement, Parks Canada – Wood Buffalo National Park, Third Party Recoveries;
- Regulatory Revenue – Airports – Landing and other fees, Inspection Services – Boiler Registration and Permits, Road Licensing and Safety (Exams & Certifications, License and other fees, Permits and Registrations and Toll Permits);
- Services and Miscellaneous – Airport concession, Sale of Heat Supply, Sale of Surplus Assets, Water/Sewer Maintenance.

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

- Revolving funds net revenue is the responsibility of the established revolving funds.
- Lease revenues are the responsibility of the Commercial Development Officer and Commercial Agreements Coordinator of Real Property Services, Facilities and Properties under Asset Management.
- Program revenues are recoveries and are the responsibility of Financial Operations under Corporate Management.
- Regulatory revenue airport landing and other fees are the responsibility of the Yellowknife airport revolving fund and the regional finance officer, airport manager and airport clerk or regional superintendent.
- Regulatory revenue compliance and licensing are the responsibility of regional licensing and admin supervisors, regional financial revenue officers, regional finance and administration managers.
- Regulatory revenue tolling and permitting are the responsibility of the Yellowknife financial operations specialist and finance and administration officer.
- Services and Miscellaneous – Airport concession, Sale of Heat Supply, Sale of Surplus Assets, Water/Sewer Maintenance is the responsibility of Yellowknife airport revolving fund, INF facilities personnel and regional personnel.

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

INF 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 INF department to provide the evidence necessary to conclude on internal control effectiveness, Crowe has concluded that additional work is required by INF 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
605 – Recording Revenue		
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.	Compliant	Approved systems and procedures are documented.
610 – Establishment of Fees		
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.	Unverifiable	Rates for non-regulated items are not reviewed on a set basis. Regulated rates are reviewed every five year as per FMB direction. 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>IB610.01 Rationale for Fees Charged</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"> - pricing details; - the price/rate basis, including direct, indirect, and accounting and system costs; and, - the time period for cyclical fee reviews. <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>	Non-Compliant	The rationale for fees charged is not documented.
620 – Collection of Receivables		
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.	Unverifiable	Although the department has been rated compliant with the specifics of section IB 620.01 below, the overall 620 compliance cannot be verified due to the potential issues noted with the credit receivables with "On

Section Policy	Compliance Assessment	Reason for Non-Compliance
		Account" coding. <i>See Observation 9 below.</i>
<p>IB 620.01 Collection of Accounts Receivable</p> <p>Except as described below, an invoice must be prepared, recorded, and delivered to the debtor as soon as a receivable is created and the debtor must be given 30 calendar days from the date of the invoice to return payment to the GNWT or Public Agency.</p> <p>If payment is not received within 30 days of the date of the invoice, the responsible department or Public Agency shall attempt to collect by notifying the debtor in writing that payment is overdue and payable immediately. At this point, the debt has become an overdue receivable.</p> <p>If payment is not received during the next 30 days (i.e., within 60 days of the date of the invoice) the responsible department or Public Agency shall attempt to collect again by notifying the debtor by telephone and in writing that payment is now 30 days overdue and payable immediately.</p> <p>If payment is not received during the next 30 days (i.e., within 90 days of the date of the invoice) the overdue receivable becomes a delinquent account receivable. The responsible department or Public Agency shall: 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>Compliant</p>	<p>Revenues on account are invoiced and the debtor is provided 30 days from the date of invoice to make payment.</p> <p>FESS sends customer statements for all accounts receivable outstanding 30 days. The department reviews accounts receivable outstanding 30-90 days. Collection efforts are made on accounts receivable outstanding 30 days. When accounts receivable are outstanding 60 days the department collection efforts by making phone calls to the customers.</p> <p>The collection responsibility is assigned correctly to the collections department at 90 days at which time the department provides notes on accounts receivable outstanding 90 days to collections department.</p>

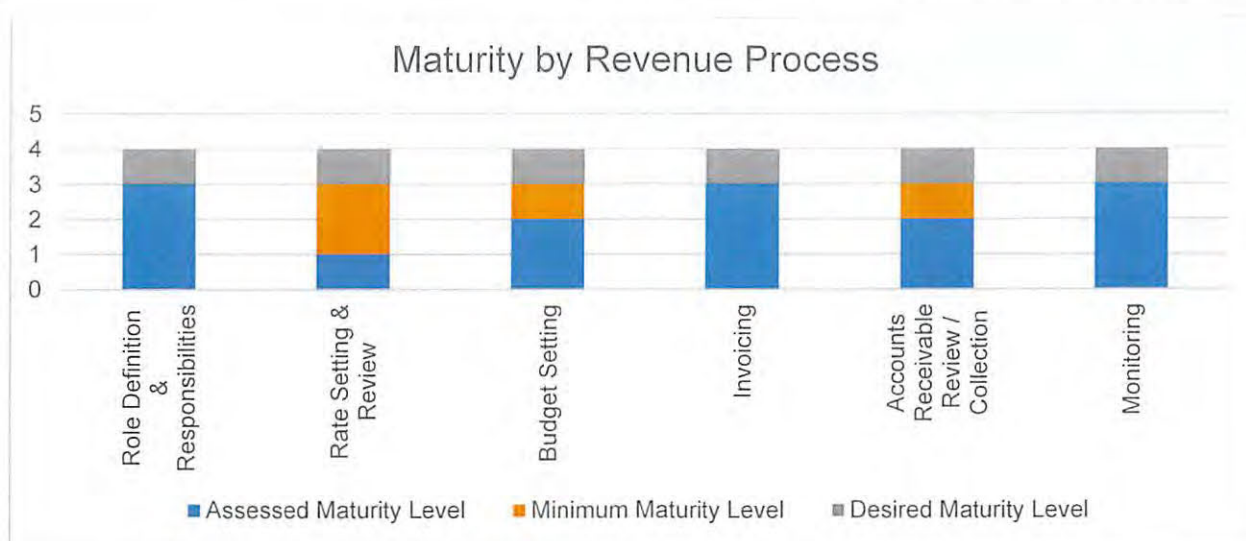
Maturity Rating Considering GNWT Internal Control Capacity Model

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 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.

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
Role Definition and Responsibilities 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"> Job descriptions exist for the positions outlined above under departmental background as responsible for the department's general revenue functions. Job descriptions include responsibilities related to specific general revenue cycle components. Job descriptions reviewed by Crowe have all been updated within the last two years.
Rate Setting & Review 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"> Majority of rates and fees are regulated and are charged in accordance with regulations. Regulated rates and fees are reviewed every five years per FMB direction. Rationale for fees is not documented. Non-regulated rates and fees are not reviewed on a set periodic basis and policies and processes are not documented. New sources of revenue are considered when new programs or initiatives are planned but a formal process does not exist.

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<i>See Observation 1, 2 and 3.</i>
<p>Budget Setting</p> <p>The department clearly defines and documents the revenues expected for each year with explanations for any material changes from prior years.</p>	Repeatable	<ul style="list-style-type: none"> • Clarity on roles and responsibilities exists for INF Financial Planning. • INF Financial Planning prepares the operating budget with revenue estimates from Corporate Services. • Budget of revenues is based on prior year estimates and actuals with input from program managers not on statistical information. • Assumptions and rationale for estimates are not documented. <p><i>See Observation 4.</i></p>
<p>Invoicing</p> <p>The department ensures that invoices are prepared in a timely manner, and are accurate and complete.</p>	Defined	<ul style="list-style-type: none"> • Invoices are not issued for the majority of the department's revenue streams because payment is received at the time of service. • Processes are in place to record revenues received in cash or by online payment at the time the service is provided. • Processes are in place to ensure all revenues earned are recorded as revenues for revenues received by cheque or direct payment. • Processes are fully documented for each significant revenue stream and are reviewed annually and updated where necessary.
<p>Accounts Receivable Review / Collection</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"> • The department has a "Finance General" email established for emails from FESS and a department representative has been assigned. • The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque. • The department has a policy for cashier functions that states application instructions are to be provided within two days to FESS for cheques received by FESS. • The policy the department has for addressing emails received from FESS regarding unallocated receipts

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<p>by cheque does not include specific procedures to be taken by department staff.</p> <ul style="list-style-type: none"> • The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting. • The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting. • The procedures to be taken when an unclaimed deposits email is received from Department of Finance - Financial Reporting have not been established and documented. • Accounts receivable are reviewed per the department's collection of current and overdue receivables policy. Collection efforts are made within the department to follow-up on balances outstanding between 30 and 90 days, with notes on collections efforts provided to Operations Manager for review. Notes are provided to Collections unit once accounts receivable are outstanding 90 days. • "On Account" balances in the department's accounts receivable are reviewed monthly as part of the accounts receivable review, as directed by the Operations Manager. • The department understands the role and responsibility of the Collections unit. • Policies mentioned above are reviewed annually and updated where necessary. <p><i>See Observations 5, 6 and 7.</i></p>
<p>Monitoring</p> <p>The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are not being received as expected.</p>	<p>Defined</p>	<ul style="list-style-type: none"> • Monthly and quarterly variances are prepared by Financial Analysts based on budgeted revenues versus actuals revenues per reports from SAM and revised projected revenues.

Revenue Process Area	Assessed Maturity Level	Findings and Comments
		<ul style="list-style-type: none"> Explanations for variances are documented. Variance reports are reviewed and provided to Management Board Secretariat. Process for variance analysis is fully documented.

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.
- The department informally reviews non-regulated rates and fees, but a policy and process has not been designed and documented for the review of all rates and fees.

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, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- a) For each revenue stream, the process established to review rates and fees should be evaluated to ensure the activities required occur on a set periodic basis that adequately addresses economical changes, which would impact the rate and fee; the process should be documented including roles and responsibilities.
- b) For regulated rates, documentation should be made to support rates are reasonable to cover the current costs associated with the services for which fees are being charged, or the rationale for rates changes.

Management Response:

Action Plan	Completion Date:
a) Corporate Services will work with program managers to document and/or develop existing processes for reviewing rates and fees.	February 29, 2020. (Note: department will make its best effort to meet this and all other dates provided subject to staff availability and priorities of Senior Management.)
b) Corporate Services will work with program managers to ensure sufficient documentation to support rates and fees charged are reasonable.	February 29, 2020

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 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:
a) The rationales on hand will be saved in DIIMS by September 30, 2019 and available for review. New processes will be added as they are developed by February 29, 2020.	February 29, 2020.

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, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Infrastructure will study formulating a policy to	Study utility of policy by December 31, 2019. Implement for next business planning cycle (2021-

satisfy this recommendation.	22).
------------------------------	------

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.
- General revenue budgets are not based on statistical information and assumptions, and rationales are not fully documented, in that unchanged amounts are not explained.

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, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- 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) Department will evaluate cost-benefit of implementing statistical processes. As noted in the interview, there are some fees, such as mechanical/electric permits that are not conducive to accurate estimates due to the volatile nature of the renovation & construction market.	December 31, 2019 for performing cost-benefit analysis for implementation and September 25, 2020 for implementation for the process, if cost-benefit analysis permits it.

Observation 5

Process for addressing unallocated cheque emails from FESS 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 INF, 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.
- INF's cashier functions policy includes a procedure to provide FESS with application instructions for cheques received by FESS but does not include procedures to be performed to determine what the cheque is for and what the application instructions should be.

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.
Risk Responsibility	Director, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations FESS

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.

Management Response:

Action Plan	Completion Date:
a) Department is implementing a new business process to ensure large payments are entered into billing so an invoice is in place for FESS to code payments against rather than posting as open items. The large payments of this nature are almost exclusively for Federal Transfer & Infrastructure Contributions.	Expected completion date by September 30, 2019.
b) FESS is working on new businesses processes to address issues with cashiers handling of unallocated cheques. They are also working with Reporting, Treasury and Risk Management to resolve issues with unallocated payments for all cheques.	FESS will need to be consulted on it.

Observation 6

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 INF revenues will be unrecorded.
Risk Responsibility	Director, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations Finance – Financial Reporting

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) The vast majority of these are Federal transfer payments, and will be resolved to the extent possible by new process by September 30, 2019, and as identified in response to Observation 5	September 30, 2019 and in line with 5 above.

Observation 7
Process for addressing unclaimed deposit emails from Financial Reporting is not documented and the process lacks procedures to be performed.

- The Manager, Financial Operations, 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, Financial Operations to the applicable department staff for review.
- If a payment is identified by department staff as being for INF, and the purpose of the receipt is known, the department staff will email the Manager, Financial Operations with the coding.
- The Manager, Financial Operations 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, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations Financial Reporting

Recommendations:

We recommend that:

- a) 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.
- b) Processes and procedures should be documented to address unclaimed deposit emails from Financial Reporting.

Management Response:

Action Plan	Completion Date:
a) Again, the majority of the dollar value is related to Federal payments. Any solution will include the Department of Finance.	Est. September 30, 2019.

b) Documentation and development of process, if required, will be completed by September 30, 2019.	Est. September 30, 2019.
--	--------------------------

Observation 8

Policy and processes have been designed and documented to address “On Account” accounts receivable, however “On Account” balances are outstanding from multiple fiscal years.

- 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 INF’s accounts receivable included \$223,385 of “On Account” credit balances from 2017/18 fiscal year and 2018/19 fiscal year, broken down as follows:
 - 2017/18 fiscal \$38,910
 - 2018/19 fiscal \$184,474
- The process designed to review “On Account” accounts receivable by the department on a regular basis does not appear to be operating effectively given the balances outstanding as at December 30, 2018.

Risk Profile:

Risk Impact	“On Account” receivables are not being addressed in a timely manner under the current process which can result in department revenue being 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, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- A review of the process should be done and specific procedures should be designed and documented that ensures “On Account” receivables are cleared monthly, when possible, and that explanations are provided for any outstanding “On Account” balances.

Management Response:

Action Plan	Completion Date:
a) We agree with the above recommendation and our existing process will be reviewed. Specific procedures will be developed and documented to strengthen our current process.	Expected to be completed by February 29, 2020.

Observation 9

Unclaimed deposits received by ConRev were not identified by INF and resulted in lost revenue to INF.

- During a review with Financial Reporting of unclaimed deposits received by ConRev posted to Finance general revenue as at March 31, 2018, it was noted that \$1,805,712.74 was recorded as Finance general revenue and then was subsequently identified by INF as receipt of INF revenues.
- The funds received were from the Government of Canada in two installments, \$1,352,539 April 1, 2017 and \$453,173.74 August 18, 2017.
- INF had recorded the revenue in 2016-17 and 2017-18 as accrued receivables.
- Financial Reporting sent an email to departments for unclaimed deposits at March 31, 2018 which included these two deposits. Financial Reporting did not receive a response from any department claiming the funds, as such, the funds were recorded as Finance general revenue.
- In 2018-19 INF identified the funds as being the receipt of the accrued AR but the funds had already been cleared to Finance general revenue; therefore the money was not assigned to INF.

Risk Profile:

Risk Impact	Revenues are misstated at the department level.
Risk Responsibility	Director, Infrastructure, Corporate Services
Risk Mitigation Support	Manager, Financial Operations

Recommendations:

We recommend that:

- a) The policy and procedures for accounts receivable be revised to include monthly review of accrued receivables.

Management Response:

Action Plan	Completion Date:
a) This is related to Federal transfer payments and will be alleviated by the processes identified above. It should be noted that the Finance section producing the Public Accounts has the final Y-E Working Papers for Accrued Receivables, and the solution to the issue should also include that they review the working papers for large dollar accruals as well, in case the emails are missed.	Expected to be completed by December 20, 2019.

APPENDIX D

DEPARTMENT OF JUSTICE

DEPARTMENT OF JUSTICE

SCOPE AND OBJECTIVES

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

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

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

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

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

DEPARTMENTAL BACKGROUND

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

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

General revenues generated by Justice consist of the following:

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

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

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

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

METHODOLOGY

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

OVERVIEW

Compliance with FAA and FAM

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

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

Based on the audit work performed, as well as the inability of the Justice department to provide the evidence necessary to conclude on internal control effectiveness, Crowe has concluded that additional work is required by Justice to design and implement internal controls to sustain an audit opinion of

“Compliant”. This will include the necessary documentation required to support that key controls are operating effectively. Support for this assessment is provided in the following table:

Section Policy	Compliance Assessment	Reason for Non-Compliance
605 – Recording Revenue		
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.	Unverifiable	Unable to verify if revenue earned is recorded in accordance with approved systems and procedures because not all significant approved systems and procedures are documented.
610 – Establishment of Fees		
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.	Unverifiable	Regulated rates are reviewed every five year as per FMB direction. The rationale for rate changes or unchanged rates at the five year review for other than inflationary changes are not documented as such it is not verifiable whether the rates address current costs of the related services or license.
<p>IB610.01 Rationale for Fees Charged</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"> - pricing details; - the price/rate basis, including direct, indirect, and accounting and system costs; and, - the time period for cyclical fee reviews. <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>	Non-Compliant	The rationale for rate changes or unchanged rates other than inflationary changes at the five year review are not documented.
620 – Collection of Receivables		
GNWT Departments and Public Agencies are responsible to collect all accounts receivable promptly, efficiently, and in a	Compliant	AR reviewed and actioned monthly

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

Section Policy	Compliance Assessment	Reason for Non-Compliance
transfer collection responsibility to the Financial Reporting and Collections Section, Finance, immediately.		

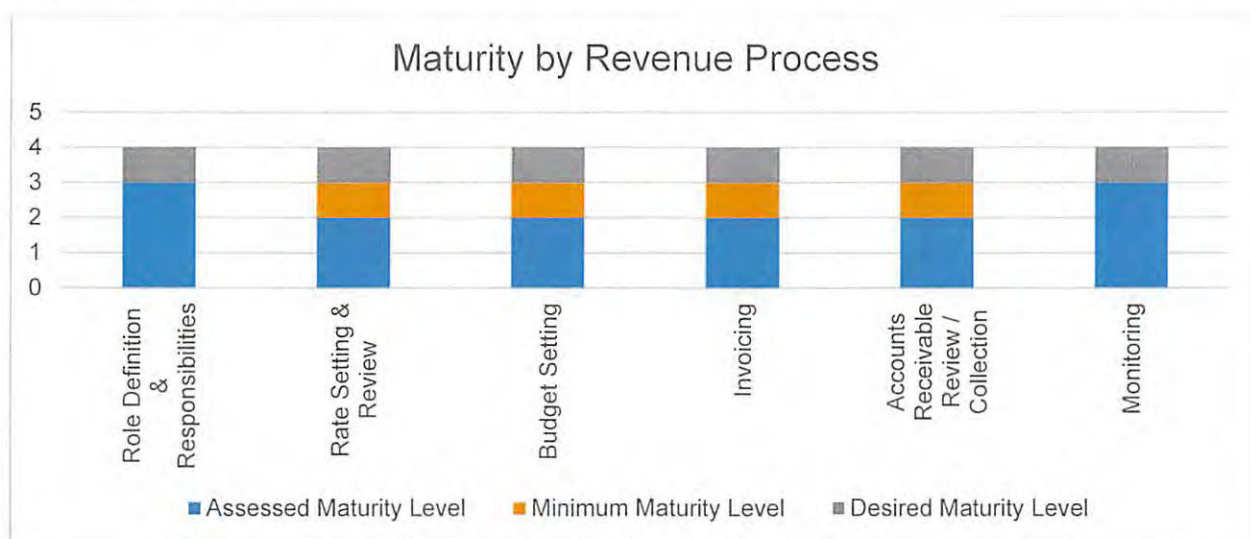
Maturity Rating Considering GNWT Internal Control Capacity Model

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

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

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

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

OBSERVATIONS AND RECOMMENDATIONS

Observation 1

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

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

Risk Profile:

<p>Risk Impact</p>	<p>Without updated job descriptions, duties, responsibilities and assignment changes may not be reflected in the job descriptions and job descriptions will not be readily available for the hiring process should a position become vacant; possibly increasing the time the</p>
--------------------	---

	position is vacant.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

Recommendations:

We recommend that:

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

Management Response:

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

Observation 2

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

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

Develop directives with respect to 5 year review of fees and associated legislation.	
--	--

Observation 3

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

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

Observation 4

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop directives for assessing new revenue sources. Share directive with program management.	June 30, 2019

Observation 5
Procedures for review of assumptions used in budget preparation are not fully documented.

- General revenues of the department are very consistent from year-to-year, or are insignificant in size.
- Procedures for review of budgeted revenues for rate changes and/or other impactful factors are not documented.

Risk Profile:

Risk Impact	A lack of documentation and review of the assumptions used in budget preparation, and lack of documentation for the process used to ensure rate changes and other impacts have been taken into account, can increase the risk of inaccurate budgeting.
Risk Responsibility	Director, Justice, Corporate Services
Risk Mitigation Support	Assistant Director, Corporate Services

Recommendations:

We recommend that:

- Procedures used to ensure that budgeted revenues are based on clearly thought out assumptions, reviewed for the impact of rate changes, or impacts to rates, should be documented and followed going forward.

Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Document procedures for development of revenue budgets.	June 30, 2019

Observation 6
Revenue processes are not fully documented.

- Processes are in place for each significant revenue stream to ensure revenues earned are recorded, but are only documented for regulatory revenues; processes for significant program revenues are not documented.

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop procedures for ensuring each major program revenue stream is accounted for.	June 30, 2019

Observation 7

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

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:

a) Management accepts this recommendation. Develop written procedures for how staff will action unallocated cheques received from FESS.	April 30, 2019
b) Management accepts this recommendations. Document processes in place for addressing the receipt of the emails from FESS relating to unallocated cheques.	

Observation 8

Processes for direct payment notifications received by department staff are not documented.

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

Risk Profile:

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

Recommendations:

We recommend that:

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

Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop written procedures for direct payment notifications.	April 30, 2019

Observation 9

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

- The Corporate Finance Officer and Assistant Director, Corporate Services, receive all emails from Financial Reporting for unclaimed deposits (direct payments received for which the purpose has not been determined by Financial Reporting).
- The email received is forwarded by Assistant Director, Corporate Services, or Corporate Finance Officer to the applicable department staff for review.
- If a payment is identified by department staff as being for Justice, and the purpose of the receipt is known, the department staff will email the Assistant Director, Corporate Services, with the coding.
- The Assistant Director, Corporate Services, provides the information received to Financial Reporting with instructions on how to apply the receipt.

- The process is not documented and specific procedures to be taken by department staff upon receipt of the unclaimed deposits email have not been designed and documented.

Risk Profile:

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

Recommendations:

We recommend that:


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

Management Response:

Action Plan	Completion Date:
a) Management accepts this recommendation. Develop written procedures with respect to management of unclaimed deposit emails from Financial Reporting.	April 30, 2019
b) Management accepts this recommendation. Develop written procedures to address emails from Financial Reporting in relation to unclaimed deposits	April 30, 2019

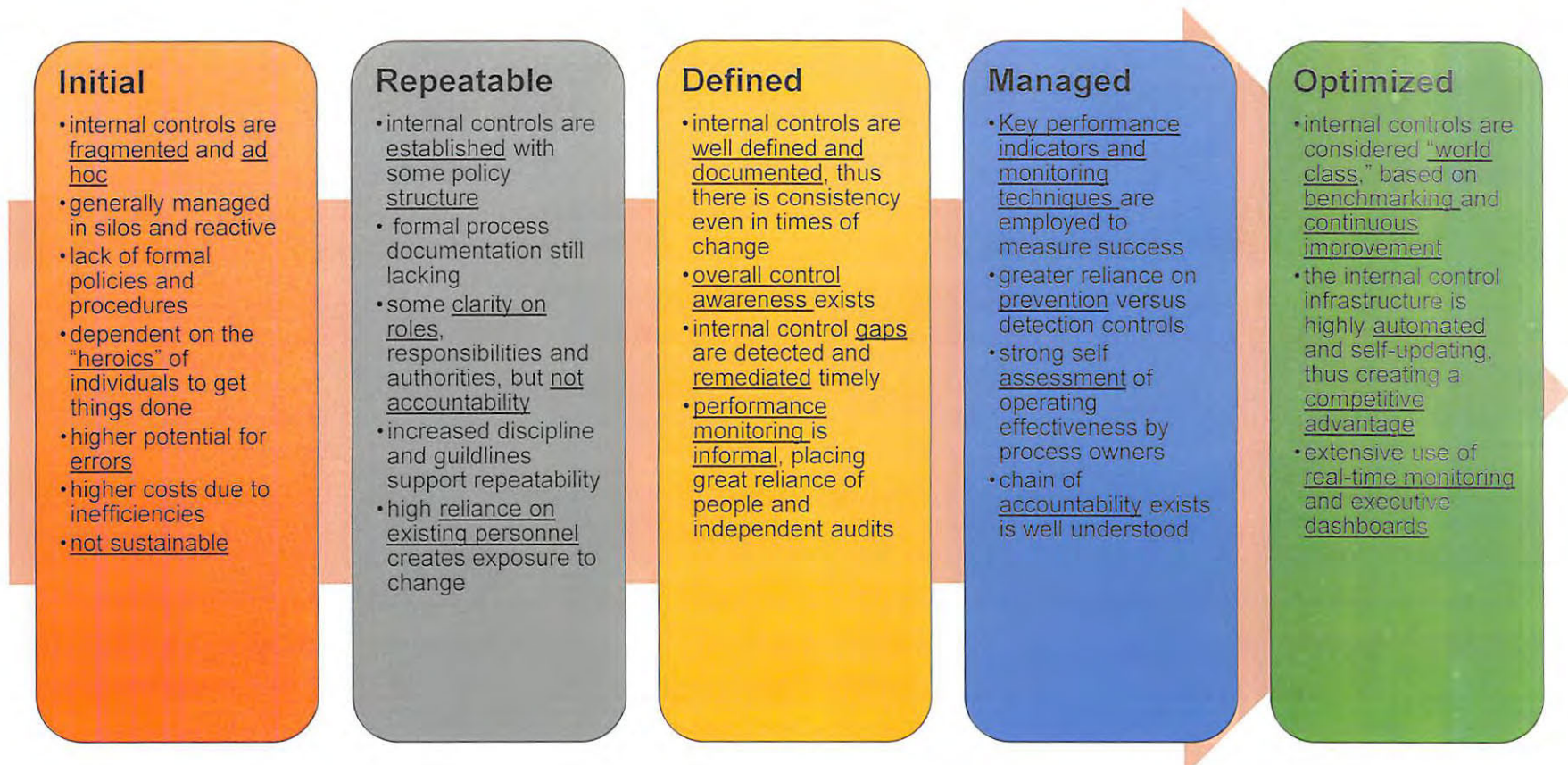
APPENDIX E

INTERNAL CONTROL CAPACITY MODEL

	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"> The organization lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of internal control assurance. Management and employees have an overall lack of awareness of internal controls.
1 - Initial/Ad Hoc - Unreliable	<p>Unpredictable environment for which controls have not been designed or implemented.</p> <ul style="list-style-type: none"> Controls are fragmented and ad hoc. Controls are 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 and higher costs due to inefficiencies. Controls are not sustainable. Individual expertise in assessing internal control adequacy is applied on an ad hoc basis. Management has not formally assigned responsibility for monitoring the effectiveness of internal controls.
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"> Controls are established with some policy structure. Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. Formal process documentation is still lacking. Some clarity on roles and responsibilities, but not on accountability. Increased discipline and guidelines support repeatability. High reliance on existing personnel creates exposure to change. Internal control assessment is dependent on the skill sets of key individuals.
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"> Controls are well-defined and documented, thus there is consistency even in times of change. Overall control awareness exists. Policies and procedures are developed for assessing and reporting on internal control monitoring activities. A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers. Control gaps are detected and remediated timely. Performance monitoring is informal, placing great reliance on the diligence of people and independent audits

Deliverable	Description
	<ul style="list-style-type: none"> • Management supports and institutes internal control monitoring. • An education and training program for internal control monitoring is defined. • Tools are being utilized but are not necessarily integrated into all processes.
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"> • Key Performance Indicators (KPIs) 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 and is well-understood. • Management implements a framework for internal control monitoring. • A formal internal control function is established, with specialized and certified professionals utilizing a formal control framework endorsed by senior management. • Skilled staff members are routinely participating in internal control assessments. • A metrics knowledge base for historical information on internal control monitoring is established. • Peer reviews for internal control monitoring are established. • Tools are implemented to standardize assessments and automatically detect control exceptions.
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"> • Controls are considered "word class", based on benchmarking and continuous improvement. • The control infrastructure is highly automated and self-updating, thus creating a competitive advantage. • Extensive use of real-time monitoring and executive dashboards. • Management establishes an organization wide continuous improvement program that takes into account lessons learned and industry good practices for internal control monitoring. • The organization uses integrated and updated tools, where appropriate, that allow effective assessment of critical controls and rapid detection of control monitoring incidents. • Benchmarking against industry standards and good practices is formalized.





CONFIDENTIAL

October 5, 2020

File: 7820-20-GNWT-151-139

MR. SANDY KALGUTKAR
DEPUTY MINISTER
FINANCE

Audit Report: Expense Data Analysis, Phase I: Duplicate Invoice Payments
Audit Period: April 1, 2016 to November 30, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the data analysis of the Government of the Northwest Territories (GNWT) departmental expenditures to assess compliance with the Financial Administration Manual (FAM) directives. The audit scope was all departmental expenditure transactions processed between April 1, 2016, and November 30, 2019, that could be tested for compliance with FAM using data analysis.

The audit analysis was divided into various phases, such as duplicate invoice payments and timing of payments. This report covers issues related to duplicate invoices paid through the GNWT's accounts payable process.

B. BACKGROUND

The GNWT disbursed approximately \$2 billion annually on operating and capital expenses. During the audit period, the GNWT processed over 390,000 accounts payable transactions totalling over \$7.2 billion.

The Financial Employee Shared Services (FESS) was responsible for processing payments for all the GNWT departments through the System for Accountability and Management (SAM) Accounts Payable (AP) module. Vendors were to send their invoices directly to FESS for payment. FESS required the department's expenditure authority to verify the invoice before processing payment. Each department was responsible for spending within its budget.

C. OVERVIEW

SAM application performed a three-way control designed to detect duplicate invoices based on the date, amount and number indicated on the invoice. Over 99.9% of the transactions were processed accurately through SAM.

Data analysis of 390,000 AP transactions identified 132,000 potential duplicates valued at \$2 billion based on the same Paid Amount and Supplier ID#. This potential duplicate population was normalized by excluding recurring payment transactions and payments less than \$500. The 22,600 normalized potential duplicates were subjected to in-depth manual examination to identified nearly 300 transactions that were highly likely to be potential duplicates (**Schedule II Refers**).

Of the 298 potential duplicates, the departments confirmed that 45% (132 of 298) of the transactions, totalling over \$800,000, were duplicates (**Schedule II Refers**). The analysis did not take into account duplicates already identified by departments and any subsequent recovery of these duplicate payments.

While a tiny number of duplicate invoice transactions were identified, the large volume of transactions processed through SAM resulted in a continuous impact of several thousands of dollars. In consideration of this and other issues identified through data analysis, the Office of the Comptroller General agreed to work with the Director of Finance and Administration community to implement internal controls to avoid duplicate payments. Consideration will also be given to implementing detective controls, such as data analysis, to identify incorrect disbursements promptly.

D. ACKNOWLEDGEMENT

We want to thank the Departmental Directors of Finance and Administration, the Department of Finance SAM team and FESS for their assistance and co-operation throughout this phase of the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

**Department of Finance
GNWT Expense Data Analysis
7820-20-GNWT-151-139**

SCHEDULE I

Observation 1: Duplicate SAM Accounts Payable Invoices

Criteria:

Financial Administration Act (FAA) 90. (1) – an expenditure officer must certify expenditures and an accounting officer must approve the expenditure amount is accurate

Financial Administration Manual (FAM) 705 – Deputy Heads must ensure all procurement transactions are properly justified, authorized, appropriated, and recorded

FAM 750 – GNWT Departments or Public Agency overpayments shall be invoiced and coded against the original expenditure in the same fiscal year or to the recovery of prior year expense if discovered in another fiscal year

Financial Employee Shared Services (FESS) Business Process – provides P2P procedures on how to process accounts payable payments

Condition/Evidence:

FAA and FAM provided the framework for improved accountability, transparency, and fiscal responsibility. FESS Business Process provided the procedures on how to process invoices for payment, and SAM application has the 3-way check control based on invoice number, amount, and date to detect duplicate.

We used data analysis to assess the 390,000 accounts payable (AP) transactions from April 1, 2016 to November 30, 2019. Our examination identified 132,000 potential duplicates valued at \$2 billion. These duplicates were based on the Paid Amount and Supplier ID#. After excluding recurring payment transactions and amounts less than \$500, we had over 25,000 normalized duplicates. After a manual review of those 25,000 transactions, we selected nearly 300 potential duplicates and requested the departments to confirm if they were actual duplicates. **(Schedule II Refers)**

Of the 298 transactions examined, the departments confirmed that 45% (132 of 298) transactions were duplicates totaling over \$800,000. **(Schedule II Refers)**. The duplicates had either:

- exact invoice number and vendor name, which may be due to allowing an override when a duplicate warning appears
- nearly identical invoice number and vendor name, which may be due to data input error on the invoice number, duplicate and inconsistent vendors in SAM, or neglecting search for duplicates before entering invoices for payment.

The examination of invoices and supporting documents was beyond the scope of data analysis. Our analysis did not take into account any recovery of duplicate payments.

**Department of Finance
GNWT Expense Data Analysis
7820-20-GNWT-151-139**

SCHEDULE I

Risk/Consequence:	
<ul style="list-style-type: none"> • Duplicate payments made to vendors resulting in: <ul style="list-style-type: none"> ○ Loss of public funds ○ Allocation of time to investigate and correct errors ○ Adverse publicity resulting in loss of public trust ○ Negative impact on GNWT cash flow even if the overpayment is corrected • External fraud by vendors 	<p>Risk Rating: High Likelihood: Almost Certain Impact: Moderate Risk Owner: Comptroller General, Finance</p> <p>Support:</p> <ul style="list-style-type: none"> • Assistant Comptroller General, Finance • Executive Director, FESS, Finance • Department DFA's
Recommendations:	
<p>We recommend the Comptroller General:</p> <ol style="list-style-type: none"> 1. Engage the DFA community to develop a coordinated plan to recover any excess payments 2. Incorporate a standard method to process recoveries of overpayment in FAM 3. Engage the FESS to consider adding more specific instructions in their business processes on accounts payable, especially on data entry of invoice numbers. 4. Assign an operating unit the responsibility of implementing detective controls, such as the use of data analytics, to detect duplication of payments through SAM's AP. 	
Management Response:	Timeline
<p>The Comptroller General will:</p> <ol style="list-style-type: none"> 1. Collaborate with the DFA community to confirm duplicates, correct records, and start the process to collect overpayments 2. Formally appraise the current FAM provision for recovery of overpayment with the possibility and intention of instituting changes to meet current situations 3. Review FESS Business Process policies and procedures for possible updates and improvements 4. Enquire into the possibility of additional preventive and detective controls within the SAM application system 	<p>December 2020</p> <p>December 2020</p> <p>December 2020</p> <p>December 2020</p>

**Department of Finance
GNWT Expense Data Analysis
7820-20-GNWT-151-139**

SCHEDULE II

GNWT departments Summary of Accounts Payable duplicate findings (VOLUME)

Dept.	Total Transactions Examined	Identified Potential Duplicates	Normalized Duplicates	Final Duplicates for Confirmation	False Positives	Confirmed Duplicates	Unverified Findings
ECE	73,679	2,206	1,209	28	20	4	4
ENR	29,562	8,655	1,921	38	20	18	-
EXE	2,399	961	172	14	-	14	-
FIN	29,832	13,006	3,093	44	20	22	2
HSS	26,640	11,520	2,024	22	10	12	-
INF	172,309	73,099	8,309	78	48	30	-
ITI	15,263	4,814	1,488	26	16	8	2
JUS	24,703	9,732	3,009	38	20	16	2
LEG	6,584	3,442	1,586	2	-	2	-
LND	2,540	508	145	6	2	4	-
MAC	7,409	4,107	2,151	2	-	2	-
Total	390,920	132,050	25,107	298	156	132	10
				100%	52%	45%	3%

GNWT departments Summary of Accounts Payable duplicate findings (Dollar Value)

Dept.	Total Transactions Examined	Identified Potential Duplicates	Normalized Duplicates	Final Duplicates for Confirmation	False Positives	Confirmed Duplicates	Unverified Findings
ECE	\$ 970,000,000	\$233,000,000	\$ 11,000,000	\$ 219,000	\$ 211,000	\$ 4,000	\$ 4,000
ENR	257,000,000	74,000,000	21,000,000	297,000	105,000	192,000	-
EXE	18,000,000	7,000,000	2,000,000	79,000	-	79,000	-
FIN	1,741,000,000	182,000,000	51,000,000	264,000	93,000	170,000	1,000
HSS	1,734,000,000	907,000,000	153,000,000	97,000	41,000	56,000	-
INF	1,497,000,000	184,000,000	57,000,000	353,000	214,000	139,000	-
ITI	125,000,000	46,000,000	12,000,000	56,000	27,000	14,000	14,000
JUS	223,000,000	63,000,000	61,000,000	199,000	46,000	141,000	12,000
LEG	23,000,000	9,000,000	5,000,000	1,000	-	1,000	-
LND	24,000,000	2,000,000	1,000,000	4,000	1,000	3,000	-
MAC	587,000,000	358,000,000	206,000,000	4,000	-	4,000	-
Total	\$7,200,000,000	\$2,065,000,000	\$580,000,000	\$ 1,573,000	\$ 738,000	\$ 803,000	\$ 31,000
				100%	47%	51%	2%



CONFIDENTIAL

June 10, 2020

File: 7820-30-GNWT-151-139

MR. SANDY KALGUTKAR
DEPUTY MINISTER
FINANCE

Audit Report: Expense Data Analysis – Phase II: Cross Department Duplicates
Audit Period: April 01, 2016 to November 30, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the data analysis of the Government of the Northwest Territories (GNWT) departmental expenditures to assess compliance with the Financial Administration Manual (FAM) directives. The audit scope was all departmental expenditure transactions processed between April 1, 2016, and November 30, 2019 that could be tested for compliance with FAM using data analysis.

The audit analysis was divided into various phases such as duplicate VISA transactions, invoicing errors, and timing of payments. This report covers issues related to duplicated payments across multiple departments.

B. BACKGROUND

The GNWT annually disbursed approximately \$2 billion on operating and capital expenses. For the audit period, over \$7.2 billion was disbursed and 390,000 accounts payable transactions processed.

The Financial Employee Shared Services (FESS) was responsible for processing payments for all the GNWT departments through the System for Accountability and Management (SAM) Accounts Payable (AP) module. Vendors could send their invoices directly to FESS or to the departments for payment. FESS required the department's expenditure authority to verify the invoice before processing a payment. Each department was responsible for spending within its budget.

C. OVERVIEW

SAM application performed a three-way control designed to detect duplicate invoices based on the invoice date, amount, and date. Our review showed that the SAM controls were effective in identifying duplicate transactions within a specific department. Over 99% of the transactions were processed accurately.

SAM did not have any controls to identify invoices that may have been paid by multiple departments. Data analysis identified 609 or 0.16% potential duplicate transactions out of the 390,000 accounts payable transactions were paid by more than one department.

An in-depth examination of potential duplicates showed that 16% (98 of 609) of the payments, totalling over \$400,000, were made by two departments for the same invoice (**Schedule I Refers**). Our analysis did not take into account any subsequent recovery of duplicate payments.

The Office of the Comptroller General agreed to take action that will mitigate the design weakness in SAM by considering additional preventive and detective controls including data analysis to identify incorrect disbursements in a timely manner.

D. ACKNOWLEDGEMENT

We want to thank the Department of Finance's Shared Corporate Services and SAM team for their assistance and co-operation throughout this phase of the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Observation 1: Duplicate Invoice Payments across Departments

Criteria:
<ul style="list-style-type: none">• No person shall incur expenditure on behalf of the Government unless an expenditure officer certifies that the expenditure is being incurred pursuant to an appropriation, and an accounting officer certifies that the amount of the expenditure is accurate- <i>Financial Administration Act 90. (1)</i>• Deputy Heads must ensure all procurement transactions are properly justified, authorized, appropriate and recorded- <i>Financial Administration Manual 705</i>• Recoveries related to an overpayment by a GNWT Department or Public Agency shall be invoiced promptly and coded against the account to which the expenditure was charged if discovered in the same fiscal year, or to Recovery of Prior Year Expense if discovered in a subsequent fiscal year – <i>Financial Administration Manual 750</i>
Condition / Evidence
<p>Accuracy and validity of payments were reliant on business process controls such as authorizations by expenditure and accounting authorities and SAM application controls. SAM application controls were designed to detect duplicate invoices based on the invoice date, amount, and number, within a specific department or business unit. This control did not apply across business units and would not identify an invoice paid by more than one department.</p> <p>The GNWT processed over 390,000 transactions over the audit period. To verify whether any invoices were paid by more than one department, we used a data analysis tool to identify payments made on invoices with the same date, invoice number, paid amount, and supplier ID. The data analysis identified 609 potential duplicate transactions.</p> <p>Over 15% (98 of 609) transactions were identified as a cross-departmental duplicate once false positives transactions such as lease payments, parking payments, and amounts below \$500 were eliminated. Specifically:</p> <ul style="list-style-type: none">i. 24 invoices were paid by two departments resulting in an additional \$306,000 paid out to Vendors. We confirmed that these were actual duplicate payments by reviewing the attached supporting invoices and documents within the SAM AP module. (Schedule II refers)ii. 25 invoices were potentially paid by two departments, which may have resulted in over \$175,000 overpaid to vendors. We were unable to verify these transactions as the supporting documents were not attached in SAM. (Schedule III refers)

Our analysis did not take into account any recovery of overpayment made by the departments or adjustments made by vendors/suppliers in subsequent invoicing to departments to reflect the overpayment. In discussion with the Department of Finance SAM Team and the Finance Managers, overpayments could be corrected in several ways. The departments would have to investigate each set of duplicate transactions. The department staff were in the best position to determine if any overpayment had been recovered as they had full access to all the supporting documentation and corporate knowledge to recall the event.

Risk/Consequence:

<ul style="list-style-type: none"> • Duplicate payments made to vendors resulting in: <ul style="list-style-type: none"> ○ Loss of public funds ○ Allocation of staff time to investigate and correct transactions ○ Adverse publicity resulting in loss of public trust ○ Negative impact on GNWT cash flow even if the overpayment is corrected • External fraud by vendors 	<p>Risk Rating: High Likelihood: Almost Certain Impact: Moderate Risk Owner: Comptroller General, Finance Support:</p> <ul style="list-style-type: none"> • Assistant Comptroller General, Finance • Executive Director, FESS, Finance • Executive Director, ERP, Finance • Department DFA's
--	---

Recommendations:

We recommend that the Comptroller General:

1. Engage the DFA community to review the cross-departmental duplicate payments and develop a coordinated plan to recover any excess payments
2. Incorporate an updated standard method to process recoveries in FAM.
3. Develop a business plan with the support of subject matter experts, such as Oracle, to assess the feasibility of implementing preventive controls in SAM to avoid future cross-department duplicates.
4. Assign an operating unit the responsibility of implementing detective controls, that considers tools such as data analytics, to avoid future cross-department duplicates.

**Department of Finance
GNWT Expense Data Analysis
7820-30-GNWT-151-139**

Management Response:	Timeline:
<p>The Comptroller General will:</p> <ol style="list-style-type: none"> 1. Work with DFAs to remove false positive from the duplicate listing of payments. 2. Direct DFAs to confirm cross-departmental duplicate payments and start the process to recover excess payments for payments. 3. Review the current FAM procedures and develop a standardized process to recovery excess payment across GNWT to be incorporated into FAM. 4. Assess the feasibility of configuring additional preventive controls within SAM 5. Implement detective controls such as data analysis, to identify and correct cross-departmental duplicate overpayments in a timely fashion to be reported to departments for action 	<p>October 31, 2020 October 31, 2020</p> <p>November 30, 2020</p> <p>August 31, 2020 August 31, 2020</p>

Summary of Confirmed Duplicates

Unit	Supplier ID	NAME	Invoice Date	Invoice Number	Paid Amount	ECE	ENR	EXE	FIN	HSS	INF	ITI	JUS	LEG	LND	MAC		
INF01	24(1)(a)(i)(B), (ii) and (iii) (B)		2017-12-14	515	14,248.96						14,248.96							
ECE01			2017-12-14	515	14,248.96	14,248.96												
ENR01			2017-12-12	1807	5,165.00			5,165.00										
ITI01			2017-12-12	1807	5,165.00								5,165.00					
HSS01			2017-12-20	2006	1,197.00							1,197.00						
JUS01			2017-12-20	2006	1,197.00										1,197.00			
HSS01			2017-12-20	2007	684.00							684.00						
JUS01			2017-12-20	2007	684.00										684.00			
MAC01			2018-11-30	4840	4,002.17													4,002.17
INF01			2018-11-30	4840	4,002.17								4,002.17					
ENR01			2018-10-06	6595	13,096.42			13,096.42										
INF01			2018-10-06	6595	13,096.42								13,096.42					
INF01			2018-11-30	9864	2,517.98								2,517.98					
EXE01			2018-11-30	9864	2,517.98					2,517.98								
INF01			2019-04-30	9954	569.00								569.00					
ITI01			2019-05-23	9954	569.00									569.00				
INF01			2018-03-05	29890	1,651.20								1,651.20					
ENR01			2018-05-03	29890	1,651.20			1,651.20										
ENR01			2018-02-12	31601	17,760.00			17,760.00										
ITI01			2018-02-12	31601	17,760.00									17,760.00				
INF01			2018-01-31	39249	36,698.41								36,698.41					
HSS01			2018-01-31	39249	36,698.41							36,698.41						
ITI01			2018-09-14	264676	1,000.00									1,000.00				
INF01			2018-09-14	264676	1,000.00								1,000.00					
MAC01			2018-05-29	267836	585.00													585.00
INF01			2018-05-29	267836	585.00								585.00					
EXE01			2018-02-28	319198	540.00					540.00								
ITI01			2018-02-28	319198	540.00									540.00				
ENR01			2019-09-12	483461	2,025.00			2,025.00										
INF01			2019-09-12	483461	2,025.00								2,025.00					
ENR01			2018-01-25	569154	501.60			501.60										
INF01			2018-01-25	569154	501.60								501.60					
MAC01			2018-02-15	604968	43,550.39													43,550.39
FIN01			2018-02-15	604968	43,550.39						43,550.39							
FIN01			2018-09-30	856093	5,250.00						5,250.00							
JUS01			2018-09-30	856093	5,250.00										5,250.00			
FIN01			2017-12-20	1416081	122,120.25						122,120.25							
INF01			2017-12-20	1416081	122,120.25								122,120.25					
FIN01			2019-08-30	2019-18	1,129.03						1,129.03							
EXE01			2019-08-30	2019-18	1,129.03					1,129.03								
INF01			2018-02-13	334 507	614.04								614.04					
ECE01			2018-02-13	334 507	614.04			614.04										
ITI01			2019-03-13	4341-02	1,155.00									1,155.00				
ENR01			2019-03-13	4341-02	1,155.00				1,155.00									
FIN01			2018-11-06	IN000009473	18,996.32						18,996.32							
HSS01			2018-11-06	IN000009473	18,996.32							18,996.32						
ENR01			2018-05-31	JC474	11,922.31				11,922.31									
MAC01			2018-05-31	JC474	11,922.31													11,922.31
			Total Amount		\$ 613,958.16	\$ 14,863.00	\$ 53,276.53	\$ 4,187.01	\$ 191,045.99	\$ 57,575.73	\$ 199,630.03	\$ 26,189.00	\$ 7,131.00	\$ -	\$ -	\$ 60,059.87		
			Total Count		48	2	8	3	5	4	13	6	3	0	0	4		

Summary of Potential Duplicates

Unit	Supplier ID	NAME	Voucher_ID	Invoice Date	Invoice_Number	Paid_Amount
INF01	24(1)(a)(i)(B), (ii) and (iii)(B)		10894	2017-05-30	26	600.00
ECE01			186755	2017-05-30	26	600.00
FIN01			33361	2017-04-07	218	1,000.00
HR001			28762	2017-04-07	218	1,000.00
HR001			28715	2017-03-10	2866	1,000.00
FIN01			33407	2017-03-10	2866	1,000.00
PWS01			391946	2016-10-31	12472	1,710.40
INF01			27873	2017-10-31	12472	1,710.40
DOT01			54655	2016-11-30	21230	3,528.57
PWS01			394111	2016-11-30	21230	3,528.57
PWS01			405749	2017-03-08	21381	620.00
DOT01			56636	2017-03-08	21381	620.00
PWS01			388898	2016-11-02	49035	3,464.58
INF01			18492	2016-11-02	49035	3,464.58
PWS01			401925	2017-02-13	51758	2,640.00
ITI01			75238	2017-02-13	51758	2,640.00
PWS01			398671	2017-01-24	96860	3,032.76
INF01			42959	2017-01-24	96860	3,032.76
PWS01			398669	2017-01-24	96872	720.67
INF01			42962	2017-01-24	96872	720.67
PWS01			409062	2017-02-28	213011	3,795.09
INF01			12682	2017-02-28	213011	3,795.09
ITI01			75200	2017-01-31	307426	886.25
EXE01			5102	2017-01-31	307426	886.25
INF01			62949	2018-05-08	639314	11,385.75
FIN01			44898	2018-05-08	639314	11,385.75
PWS01			395292	2016-12-16	781196	3,074.80
INF01			32253	2016-12-16	781196	3,074.80
MAC01			16619	2017-03-12	15570894	2,392.76
FIN01			32863	2017-03-12	15570894	2,392.76
ENR01			89925	2017-09-12	16680514	43,056.26
INF01			25044	2017-09-12	16680514	43,056.26
INF01			28513	2017-09-26	17082721	690.06
ITI01			79558	2017-09-26	17082721	690.06
INF01			99961	2019-05-17	20454361	28,674.00
ECE01			225742	2019-05-17	20454361	28,674.00
ECE01			229736	2019-09-17	21170984	46,189.80
INF01			112253	2019-09-17	21170984	46,189.80
FIN01			38046	2017-09-29	24919152	875.45
INF01			31405	2017-09-17	24919152	875.45
ITI01	70202	2016-03-21	16-285	3,914.80		
FIN01	25206	2016-03-21	16-285	3,914.80		
PWS01	362966	2016-04-05	2012-1422	4,956.00		
HSS01	52246	2016-04-05	2012-1422	4,956.00		
LEG01	12985	2017-02-21	G3727	2,553.91		
ECE01	184858	2017-02-21	G3727	2,553.91		
EXE01	4721	2016-03-28	IN00023819	3,722.00		
PWS01	363132	2016-03-28	IN00023819	3,722.00		
ENR01	78589	2016-10-26	IN174406	872.08		
PWS01	388761	2016-10-26	IN174406	872.08		
				Total Amount		\$ 350,711.98
				Total Count		50



CONFIDENTIAL

October 6, 2020

File: 7820-20-GNWT-151-139

MR. SANDY KALGUTKAR
DEPUTY MINISTER
FINANCE

Audit Report: Expense Data Analysis, Phase III: Duplicate Account Payable
Audit Period: April 1, 2016 to November 30, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the data analysis of the Government of the Northwest Territories (GNWT) departmental expenditures to assess compliance with the Financial Administration Manual (FAM) directives. The audit scope was all departmental expenditure transactions processed between April 1, 2016, and November 30, 2019, that could be tested for compliance with FAM using data analysis.

The audit analysis was divided into various phases, such as duplicate Visa transactions, invoicing errors, and timing of payments. This report covers issues related to duplicate payments processed through the GNWT's accounts payable process.

B. BACKGROUND

The GNWT disbursed approximately \$2 billion annually on operating and capital expenses. During the audit period, the GNWT processed over 390,000 accounts payable transactions totalling over \$7.2 billion. Concurrently, the GNWT processed over 375,000 Corporate Credit Card (Visa) transactions totalling over \$158 million.

The Financial Employee Shared Services (FESS) was responsible for processing payments for the GNWT departments through the System for Accountability and Management (SAM) Accounts Payable (AP) module. FESS was expected to process AP payments over \$10,000, while payments under \$10,000 were usually to be processed by departments using Visa unless the vendor did not accept Visa or the payment was related to a purchase order.

Vendors were to send their invoices directly to FESS for payment. FESS required the department's expenditure authority to verify all invoices before processing a payment in SAM.

C. OVERVIEW

SAM application performed a three-way control designed to detect duplicate invoices based on the date, amount and number indicated on the invoice. Over 99% of the transactions were processed accurately within departments.

SAM did not have any controls to identify invoices that may have been paid by Visa. Departments were to implement manual internal controls to ensure that duplicate payments were not made through SAM and Visa. Using data analysis in reviewing 390,000 AP and 375,000 Visa transactions, valued between \$1,000 and \$10,000, we identified over 32,400 or 4% potential duplicate transactions where the same amount was paid by SAM and Visa.

An in-depth examination showed that less than 1% (303 of 32,400) of the payments, totalling over \$850,000, were potential duplicates with the same amount paid, similar vendor name and transaction date (**Schedule I Refers**). The majority of the duplicate payments were processed in the same department, while a few transactions had been processed by two departments. The analysis did not take into account duplicates already identified by departments and any subsequent recovery of these duplicate payments.

The Office of the Comptroller General agreed to work with the Director of Finance and Administration community to implement internal controls to avoid

duplicate payment through SAM and Visa. Consideration will also be given to implementing detective controls, such as data analysis, to identify incorrect disbursements promptly.

D. ACKNOWLEDGEMENT

We want to thank the Department of Finance Reporting, Treasury & Risk Management Division's Financial Reporting section and the SAM team for their assistance and co-operation throughout this phase of the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Observation: Phase III, Duplicate Accounts Payable Payments by SAM and Visa

Criteria:

- **Financial Administration Act 90. (1):** expenditures must be certified by an expenditure officer and an accounting officer must certify the expenditure amount is accurate
- **Financial Administration Manual (FAM) 705:** Deputy Heads to ensure procurement transactions are properly justified, authorized, appropriate and recorded
- **FAM 730:** Corporate Credit Cards are the primary method of payment for authorized purchases of goods and services up to \$10,000
- **FAM 750:** GNWT Departments or Public Agency overpayments shall be invoiced and coded against the original expenditure in the same fiscal year or to the recovery of prior year expense if discovered in another fiscal year.

Condition / Evidence

The main internal control to ensure accurate invoice payments were expenditure and accounting authorizations as well as application controls in the System for Accountability and Management (SAM). Purchases under \$10,000 were usually processed using Corporate Credit Cards (Visa's) unless the vendor did not accept Visa payment or the invoice amount was related to a purchase order. In contrast, expenditures over \$10,000 were processed in the SAM Accounts Payable (AP) module. A control to check to identify duplicate payments through SAM and Visa did not exist.

During the audit period, the GNWT processed 766,310 (390,920 AP and 375,390 Visa) transactions. These transactions totalled approximately \$7.4 billion (\$7.2 billion AP and \$158 million Visa). To verify whether both the AP and Visa methods were used to pay the same invoice, we used a data analysis tool to identify invoices with the same amount paid. We filtered transaction amounts greater than \$1,000 and less than \$10,000 (\$363 million AP and \$80 million Visa). The data analysis identified 4% (32,400 of 766,310) of transactions totalling over \$73 million with the same amount paid by AP and Visa.

The variation of the SAM vendor name from the Visa vendor name made it difficult to detect duplicate payment transactions using a computer application. A manual examination of the *same amount, similar vendor name, and similar transaction date* identified less than 1% (303 of 32,400) of potential duplicate payments totalling \$851,000 (**Schedule II Refers**). Some items were paid by two departments (i.e. FIN and Exec or LND and ITI), but a majority were paid within a department.

Further analysis to verify whether the transactions were genuine duplicate payments or false positives was required. The departments must also consider any adjustments made by vendors/suppliers in subsequent invoicing to departments to correct the overpayment.

Risk/Consequence:	
<ul style="list-style-type: none"> • Duplicate payments made to vendors resulting in: <ul style="list-style-type: none"> ○ Accidental or intentional loss of public funds ○ Allocation of staff time to investigate and correct transactions ○ Adverse publicity resulting in loss of public trust ○ Negative impact on GNWT cash flow even if the overpayment is corrected 	<p>Risk Rating: High Likelihood: Almost Certain Impact: Moderate Risk Owner: Comptroller General, Finance Support:</p> <ul style="list-style-type: none"> • Assistant Comptroller General, Finance • Executive Director, FESS, Finance • Department DFA's
Recommendations:	
<p>We recommend the Comptroller General:</p> <ol style="list-style-type: none"> 1. Engage the DFA community to review the identified payments and confirm actual duplicate payment from false-positive transactions 2. Engage the DFA community to develop a coordinated plan to recover any excess payments 3. Incorporate a standard method to process excess recoveries in FAM 4. Engage the DFA community to develop a standard method for processing invoices under \$10,000 to prevent duplicate payments 5. Assign an operating unit the responsibility of implementing detective controls, such as the use of data analytics, to detect duplication of payments through Visa and SAM's AP. 	
Management Response:	Timeline:
<p>The Comptroller General will:</p> <ol style="list-style-type: none"> 1. Initiate communication with the DFAs to review identified payments as actual duplicate payments or false positives. 2. Initiate the work with the DFA community to recover any excess payments – departments will be responsible for the collection activity 3. Review FAM and determine if a standard process to recover payments is required 4. Collaborate with the DFA community to refine the payment process verification to ensure that payment is processed either through Visa or SAM only. 5. Implement detective controls, such as the use of data analytics, to identify and correct duplicate payments through Visa and SAM 	<p>October 2020</p> <p>October 2020</p> <p>October 2020</p> <p>October 2020</p> <p>November 2020</p>

GNWT Expense Data Analysis
7820-21-GNWT-151-139
April 1, 2016 to November 30, 2019

SCHEDULE II

Summary of Potential Duplicates (AP & VISA Payments)

#	Merchant	AP_Unit	Amount	Fiscal Year	Type	Posted	Trans Date
1	24(1)(a)(i)(B), (ii) and (iii)(B)	DOT01	1,001.70	2017	VISA	2016-07-20	2016-07-18
2		DOT01	1,001.70	2017	AP	2016-04-29	2016-04-12
3		DOT01	1,001.70	2017	AP	2016-06-23	2016-04-11
4		DOT01	1,001.70	2017	VISA	2016-04-07	2016-04-05
5		DOT01	1,003.06	2017	AP	2016-05-09	2016-04-30
6		DOT01	1,003.06	2017	VISA	2016-05-02	2016-04-30
7		INF01	1,004.30	2019	VISA	2018-11-28	2018-11-26
8		INF01	1,004.30	2019	AP	2018-11-22	2018-11-21
9		INF01	1,017.61	2019	VISA	2019-02-05	2019-02-04
10		INF01	1,017.61	2019	AP	2019-02-07	2019-01-10
11		EXE01	1,019.13	2017	VISA	2017-01-27	2017-01-26
12		EXE01	1,019.13	2017	AP	2017-01-19	2017-01-17
13		INF01	1,026.75	2019	AP	2018-10-10	2018-10-09
14		INF01	1,026.75	2019	VISA	2018-10-11	2018-10-10
15		INF01	1,035.83	2020	VISA	2019-11-11	2019-11-08
16		INF01	1,035.83	2020	AP	2019-09-19	2019-09-04
17		INF01	1,038.88	2019	VISA	2018-04-27	2018-04-25
18		INF01	1,038.88	2018	AP	2018-02-15	2018-03-01
19		ENR01	1,044.41	2018	VISA	2018-03-21	2018-03-20
20		ENR01	1,044.41	2018	AP	2018-03-15	2018-03-07
21		ENR01	1,049.28	2018	VISA	2018-02-15	2018-02-13
22		ENR01	1,049.28	2018	AP	2017-08-17	2017-07-13
23		MAC01	1,052.56	2017	AP	2017-02-24	2017-02-23
24		MAC01	1,052.56	2017	VISA	2017-03-13	2017-03-10
25		HSS01	1,065.90	2020	AP	2019-04-08	2019-04-08
26		HSS01	1,065.90	2020	VISA	2019-04-18	2019-04-17
27		INF01	1,067.40	2020	VISA	2019-10-08	2019-10-07
28		INF01	1,067.40	2020	AP	2019-10-01	2019-10-01
29		INF01	1,067.73	2020	VISA	2019-07-15	2019-07-12
30		INF01	1,067.73	2020	AP	2019-08-12	2019-07-05
31		INF01	1,069.24	2019	VISA	2018-04-19	2018-04-17
32		INF01	1,069.24	2018	AP	2018-02-23	2018-02-20
33		ENR01	1,080.75	2020	VISA	2019-10-04	2019-10-03
34		ENR01	1,080.75	2020	AP	2019-08-29	2019-08-29
35		INF01	1,094.20	2020	VISA	2019-04-05	2019-04-04
36		INF01	1,094.20	2020	AP	2019-04-03	2019-01-31
37		INF01	1,099.04	2019	VISA	2018-07-13	2018-07-11
38		INF01	1,099.04	2019	AP	2018-07-12	2018-07-12
39		ENR01	1,112.15	2018	AP	2017-12-14	2017-10-17
40		ENR01	1,112.15	2018	VISA	2017-12-21	2017-12-19
41		DOT01	1,122.03	2017	AP	2016-07-12	2016-07-07
42		DOT01	1,122.03	2017	VISA	2016-07-08	2016-07-07
43		ENR01	1,128.25	2017	VISA	2016-04-27	2016-04-26
44		ENR01	1,128.25	2017	AP	2016-04-12	2016-04-12
45		ECE01	1,132.56	2020	VISA	2019-06-19	2019-06-18
46		ECE01	1,132.56	2020	VISA	2019-07-11	2019-07-10
47		ECE01	1,132.56	2020	VISA	2019-08-16	2019-08-15
48		ECE01	1,132.56	2020	AP	2019-07-12	2019-07-03
49		ECE01	1,132.56	2020	AP	2019-07-19	2019-07-17
50		INF01	1,140.56	2019	VISA	2018-11-27	2018-11-26
51		INF01	1,140.56	2019	AP	2018-11-22	2018-10-31
52		INF01	1,158.25	2020	VISA	2019-07-03	2019-07-02
53		INF01	1,158.25	2020	AP	2019-06-14	2019-06-14
54		INF01	1,173.64	2019	VISA	2018-07-13	2018-07-12
55		INF01	1,173.64	2019	AP	2018-05-14	2018-04-27
56		JUS01	1,195.58	2019	VISA	2018-06-04	2018-06-01
57		JUS01	1,195.58	2018	AP	2018-02-16	2018-02-16
58		JUS01	1,195.58	2019	AP	2018-08-27	2018-08-17
59		INF01	1,201.18	2018	VISA	2018-02-26	2018-02-23
60		INF01	1,201.18	2018	AP	2018-02-19	2018-02-19
61		ENR01	1,207.50	2018	VISA	2018-01-17	2018-01-16
62		ENR01	1,207.50	2018	VISA	2018-01-17	2018-01-16
63		ENR01	1,207.50	2018	AP	2018-01-19	2018-01-16
64		ENR01	1,207.50	2018	AP	2018-01-19	2018-01-16

GNWT Expense Data Analysis
7820-21-GNWT-151-139
April 1, 2016 to November 30, 2019

#	Merchant	AP_Unit	Amount	Fiscal Year	Type	Posted	Trans_Date
65	24(1)(a)(i)(B), (ii) and (iii)(B)	ITIO1	1,211.91	2020	VISA	2019-06-12	2019-06-11
66		ITIO1	1,211.91	2019	AP	2018-08-24	2018-08-22
67		ITIO1	1,230.69	2018	VISA	2018-03-15	2018-03-13
68		ITIO1	1,230.69	2018	AP	2018-01-26	2018-01-17
69		JUS01	1,237.50	2018	AP	2018-03-15	2018-01-17
70		JUS01	1,237.50	2019	VISA	2018-07-06	2018-07-05
71		ITIO1	1,252.13	2017	VISA	2016-06-08	2016-06-08
72		ITIO1	1,252.13	2017	AP	2016-04-08	2016-01-31
73		HSS01	1,262.50	2019	VISA	2018-07-30	2018-07-25
74		HSS01	1,262.50	2019	AP	2018-07-25	2018-03-31
75		INF01	1,271.80	2019	AP	2018-11-20	2018-11-19
76		INF01	1,271.80	2019	VISA	2019-02-04	2019-02-01
77		DOT01	1,307.32	2017	VISA	2016-06-03	2016-06-02
78		DOT01	1,307.32	2017	AP	2016-05-12	2016-03-16
79		JUS01	1,312.50	2019	AP	2019-01-23	2019-01-03
80		JUS01	1,312.50	2019	AP	2019-01-23	2019-01-03
81		JUS01	1,312.50	2019	AP	2019-01-23	2019-01-03
82		JUS01	1,312.50	2019	AP	2019-01-14	2019-01-14
83		JUS01	1,312.50	2019	VISA	2019-03-06	2019-03-05
84		ECE01	1,331.25	2019	VISA	2018-08-09	2018-08-08
85		ECE01	1,331.25	2019	AP	2018-07-27	2017-12-06
86		INF01	1,370.46	2019	VISA	2018-06-12	2018-06-11
87		INF01	1,370.46	2018	AP	2018-03-28	2018-02-28
88		ENR01	1,371.50	2019	VISA	2019-01-28	2019-01-23
89		ENR01	1,371.50	2019	AP	2019-01-23	2019-01-15
90		INF01	1,375.50	2020	VISA	2019-06-19	2019-06-18
91		INF01	1,375.50	2020	AP	2019-06-14	2019-04-11
92		DOT01	1,393.20	2017	VISA	2017-03-09	2017-03-08
93		INF01	1,393.20	2018	AP	2017-06-30	2017-06-26
94		INF01	1,402.68	2020	VISA	2019-10-14	2019-10-11
95		INF01	1,402.68	2020	AP	2019-07-04	2019-06-28
96		ECE01	1,428.34	2020	AP	2019-06-05	2019-06-05
97		ECE01	1,428.34	2020	VISA	2019-06-11	2019-06-10
98		INF01	1,431.90	2018	VISA	2017-05-29	2017-05-26
99		INF01	1,431.90	2018	AP	2017-05-26	2017-05-26
100		LND01	1,437.55	2017	AP	2016-08-31	2016-08-19
101		LND01	1,437.55	2017	VISA	2016-09-01	2016-08-31
102		ECE01	1,439.85	2018	AP	2018-03-09	2017-11-08
103		ECE01	1,439.85	2019	AP	2018-05-31	2018-05-31
104		ECE01	1,439.85	2018	VISA	2018-02-26	2018-02-23
105		INF01	1,444.07	2019	AP	2019-02-21	2019-02-21
106		INF01	1,444.07	2020	VISA	2019-04-10	2019-04-09
107		INF01	1,448.28	2018	AP	2018-02-10	2018-02-10
108		INF01	1,448.28	2018	VISA	2018-03-16	2018-03-15
109		HRO01	1,496.25	2017	AP	2017-02-10	2017-02-02
110		JUS01	1,496.25	2017	AP	2017-02-23	2017-02-21
111		JUS01	1,496.25	2017	AP	2017-02-20	2017-02-02
112		HRO01	1,496.25	2017	VISA	2017-03-09	2017-03-08
113		HRO01	1,496.25	2017	VISA	2017-03-24	2017-03-23
114		HRO01	1,496.25	2017	VISA	2017-03-30	2017-03-29
115		JUS01	1,496.25	2017	VISA	2017-01-31	2017-01-30
116		JUS01	1,496.25	2017	VISA	2017-03-31	2017-03-30
117		JUS01	1,504.47	2017	VISA	2016-11-11	2016-11-10
118		JUS01	1,504.47	2017	AP	2016-10-28	2016-10-27
119		ENR01	1,529.92	2017	AP	2017-02-08	2017-01-27
120		ENR01	1,529.92	2017	VISA	2017-03-02	2017-03-01
121		ECE01	1,544.40	2020	VISA	2019-06-19	2019-06-18
122		ECE01	1,544.40	2020	AP	2019-06-12	2019-06-10
123		ECE01	1,544.40	2020	AP	2019-08-22	2019-08-19
124		INF01	1,554.74	2018	VISA	2017-11-02	2017-10-30
125		INF01	1,554.74	2018	AP	2017-10-27	2017-10-27
126		HSS01	1,563.40	2019	AP	2018-09-19	2018-09-19
127		HSS01	1,563.40	2019	VISA	2018-10-11	2018-10-10
128		INF01	1,603.15	2018	VISA	2018-02-14	2018-02-13
129		INF01	1,603.15	2018	AP	2018-01-29	2018-01-26
130		INF01	1,607.03	2020	AP	2019-06-10	2019-06-05
131		INF01	1,607.03	2020	VISA	2019-07-08	2019-07-04
132		INF01	1,621.28	2018	AP	2017-10-10	2017-08-23

GNWT Expense Data Analysis
7820-21-GNWT-151-139
April 1, 2016 to November 30, 2019

#	Merchant	AP_Unit	Amount	Fiscal Year	Type	Posted	Trans_Date
133	24(1)(a)(i)(B), (ii) and (iii)(B)	INF01	1,621.28	2018	VISA	2017-08-24	2017-08-23
134		INF01	1,657.50	2019	AP	2018-07-04	2018-07-04
135		INF01	1,657.50	2020	VISA	2019-11-13	2019-11-12
136		MAC01	1,682.84	2020	AP	2019-05-17	2019-05-08
137		MAC01	1,682.84	2020	VISA	2019-05-20	2019-05-15
138		INF01	1,722.24	2019	AP	2018-09-28	2018-09-28
139		INF01	1,722.24	2019	VISA	2019-01-04	2019-01-03
140		DOT01	1,737.66	2017	AP	2016-04-26	2016-04-11
141		DOT01	1,737.66	2017	VISA	2016-04-18	2016-04-15
142		ECE01	1,750.32	2020	VISA	2019-07-03	2019-07-02
143		ECE01	1,750.32	2020	VISA	2019-10-02	2019-10-01
144		ECE01	1,750.32	2020	AP	2019-07-19	2019-07-17
145		ECE01	1,750.32	2020	AP	2019-08-22	2019-08-16
146		INF01	1,783.20	2020	VISA	2019-09-06	2019-09-05
147		INF01	1,783.20	2020	AP	2019-08-07	2019-05-16
148		HSS01	1,795.75	2019	VISA	2019-03-18	2019-03-15
149		HSS01	1,795.75	2019	AP	2019-03-15	2019-02-28
150		DOT01	1,886.32	2017	AP	2016-09-28	2016-09-19
151		DOT01	1,886.32	2017	VISA	2016-09-20	2016-09-19
152		ENR01	1,911.90	2018	VISA	2018-01-18	2018-01-17
153		ENR01	1,911.90	2018	AP	2018-01-24	2017-11-26
154		HRO01	1,915.42	2017	VISA	2017-02-03	2017-02-02
155		HRO01	1,915.42	2017	AP	2017-01-10	2016-12-31
156		ITI01	1,922.30	2019	VISA	2019-02-28	2019-02-28
157		ITI01	1,922.30	2019	VISA	2019-02-28	2019-02-28
158		ITI01	1,922.30	2019	AP	2019-03-05	2019-02-26
159		ITI01	1,922.30	2019	AP	2019-03-05	2019-02-26
160		DOT01	1,927.80	2017	VISA	2016-04-28	2016-04-27
161		DOT01	1,927.80	2017	AP	2016-04-27	2016-04-27
162		DOT01	2,014.13	2017	VISA	2016-12-23	2016-12-23
163		DOT01	2,014.13	2017	AP	2016-12-07	2016-11-24
164		FIN01	2,021.47	2019	AP	2019-01-31	2018-12-17
165		FIN01	2,021.47	2019	AP	2019-01-31	2018-11-19
166		FIN01	2,021.47	2019	VISA	2019-02-22	2019-02-19
167		FIN01	2,021.47	2019	VISA	2019-03-29	2019-03-28
168		FIN01	2,021.47	2020	VISA	2019-04-01	2019-03-29
169		ECE01	2,061.82	2019	VISA	2018-08-10	2018-08-09
170		ECE01	2,061.82	2019	AP	2018-08-01	2018-07-11
171		JUS01	2,131.50	2018	AP	2017-05-09	2017-05-09
172		JUS01	2,131.50	2018	VISA	2017-07-20	2017-07-19
173		INF01	2,169.28	2018	VISA	2018-02-27	2018-02-23
174		INF01	2,169.28	2018	AP	2018-02-24	2018-02-20
175		INF01	2,211.62	2019	VISA	2018-04-09	2018-04-05
176		INF01	2,211.62	2018	AP	2017-06-22	2017-06-12
177		INF01	2,236.70	2019	VISA	2018-06-13	2018-06-12
178		INF01	2,236.70	2019	AP	2018-06-07	2018-03-12
179		LND01	2,259.97	2017	AP	2016-07-05	2016-06-30
180		LND01	2,259.97	2017	VISA	2016-12-15	2016-12-14
181		INF01	2,369.04	2019	VISA	2018-06-18	2018-06-14
182		INF01	2,369.04	2019	AP	2018-07-02	2018-07-02
183		INF01	2,369.04	2019	AP	2018-10-02	2018-10-02
184		ECE01	2,417.18	2020	VISA	2019-04-08	2019-04-05
185		ECE01	2,417.18	2020	AP	2019-04-25	2019-04-08
186		ITI01	2,480.19	2020	VISA	2019-04-17	2019-04-15
187		ITI01	2,480.19	2020	AP	2019-04-12	2019-04-12
188		INF01	2,543.60	2019	AP	2018-11-20	2018-11-18
189		INF01	2,543.60	2019	VISA	2018-06-21	2018-06-20
190		INF01	2,543.60	2019	VISA	2018-10-08	2018-10-05
191		INF01	2,650.24	2018	AP	2017-11-22	2017-11-14
192		INF01	2,650.24	2020	VISA	2019-05-28	2019-05-24
193		ITI01	2,662.88	2019	VISA	2018-05-11	2018-05-07
194		ITI01	2,662.88	2019	AP	2018-10-15	2018-10-15
195		INF01	2,665.40	2018	VISA	2018-03-22	2018-03-21
196		INF01	2,665.40	2018	AP	2018-03-07	2018-02-22
197		ENR01	2,681.74	2018	VISA	2018-03-27	2018-03-26
198		ENR01	2,681.74	2020	AP	2019-10-17	2018-01-31
199		ITI01	2,743.23	2019	VISA	2018-07-31	2018-07-30
200		ITI01	2,743.23	2018	AP	2018-02-28	2018-02-28

GNWT Expense Data Analysis
7820-21-GNWT-151-139
April 1, 2016 to November 30, 2019

#	Merchant	AP_Unit	Amount	Fiscal Year	Type	Posted	Trans_Date
201	24(1)(a)(i)(B), (ii) and (iii)(B)	FIN01	2,756.60	2018	AP	2018-02-16	2018-02-15
202		FIN01	2,756.60	2018	VISA	2018-02-19	2018-02-16
203		INF01	2,761.40	2019	AP	2018-06-14	2018-06-05
204		INF01	2,761.40	2019	VISA	2018-06-12	2018-06-08
205		INF01	2,795.72	2019	AP	2018-06-13	2018-06-05
206		INF01	2,795.72	2019	VISA	2018-06-12	2018-06-08
207		HSS01	2,815.56	2017	VISA	2016-09-28	2016-09-27
208		HSS01	2,815.56	2017	AP	2016-05-03	2016-04-29
209		INF01	2,872.72	2020	VISA	2019-07-26	2019-07-24
210		INF01	2,872.72	2020	AP	2019-08-29	2019-07-22
211		LND01	2,975.11	2020	VISA	2019-07-15	2019-07-12
212		ITIO1	2,975.11	2020	AP	2019-05-31	2019-05-31
213		FIN01	3,341.81	2018	AP	2018-02-06	2018-01-31
214		FIN01	3,341.81	2018	VISA	2018-02-15	2018-02-13
215		ITIO1	3,412.50	2018	VISA	2017-09-14	2017-09-13
216		ITIO1	3,412.50	2018	AP	2017-11-07	2017-10-31
217		ENR01	3,454.50	2020	AP	2019-08-01	2019-07-31
218		ENR01	3,454.50	2020	VISA	2019-08-05	2019-08-02
219		ECE01	3,455.64	2018	AP	2017-12-02	2017-11-27
220		ECE01	3,455.64	2018	VISA	2018-02-26	2018-02-23
221		ENR01	3,589.55	2019	VISA	2018-05-07	2018-05-04
222		ENR01	3,589.55	2017	AP	2017-01-05	2016-12-16
223		INF01	3,623.31	2020	VISA	2019-10-28	2019-10-25
224		INF01	3,623.31	2020	AP	2019-10-10	2019-10-10
225		HSS01	3,632.71	2018	VISA	2018-03-07	2018-03-06
226		HSS01	3,632.71	2018	AP	2018-01-09	2017-12-27
227		EXE01	3,692.06	2020	VISA	2019-06-27	2019-06-26
228		FIN01	3,692.06	2020	AP	2019-06-20	2019-06-19
229		INF01	3,878.03	2019	VISA	2018-10-12	2018-10-10
230		INF01	3,878.03	2019	AP	2018-06-22	2018-06-19
231		ITIO1	3,900.12	2019	VISA	2018-08-13	2018-08-10
232		ITIO1	3,900.12	2019	AP	2018-07-31	2018-07-31
233		INF01	3,909.30	2018	VISA	2018-03-14	2018-03-13
234		INF01	3,909.30	2018	AP	2018-03-23	2018-03-12
235		INF01	4,288.65	2019	VISA	2019-03-22	2019-03-20
236		INF01	4,288.65	2019	AP	2018-06-05	2018-05-17
237		ITIO1	4,456.35	2017	VISA	2016-11-15	2016-11-14
238		ITIO1	4,456.35	2017	AP	2016-11-22	2016-11-02
239		PWS01	4,470.64	2017	VISA	2016-06-02	2016-06-01
240		PWS01	4,470.64	2016	AP	2016-03-29	2016-03-29
241		MAC01	4,719.80	2019	VISA	2018-07-10	2018-07-09
242		MAC01	4,719.80	2019	AP	2018-06-30	2018-06-29
243		INF01	4,775.20	2018	VISA	2017-11-01	2017-10-31
244		INF01	4,775.20	2018	AP	2017-11-10	2017-11-01
245		INF01	4,804.62	2020	VISA	2019-06-21	2019-06-20
246		INF01	4,804.62	2020	AP	2019-05-31	2019-05-31
247		INF01	4,820.70	2019	VISA	2018-05-21	2018-05-16
248		INF01	4,820.70	2019	AP	2018-05-16	2018-05-16
249		INF01	4,898.87	2018	AP	2018-03-16	2018-01-12
250		INF01	4,898.87	2019	VISA	2018-04-06	2018-04-05
251		ITIO1	4,900.12	2019	VISA	2018-09-24	2018-09-21
252		ITIO1	4,900.12	2019	AP	2018-10-25	2018-09-21
253		INF01	4,930.50	2019	VISA	2018-05-24	2018-05-23
254		INF01	4,930.50	2018	AP	2017-12-11	2017-10-13
255		INF01	4,943.55	2019	VISA	2018-04-09	2018-04-05
256		INF01	4,943.55	2018	AP	2018-02-05	2018-01-12
257		JUS01	4,951.55	2018	VISA	2017-08-24	2017-08-22
258		INF01	4,951.55	2018	AP	2017-07-09	2017-07-10
259		ENR01	4,990.50	2018	VISA	2018-02-26	2018-02-23
260		ENR01	4,990.50	2018	AP	2018-02-23	2018-02-21
261		PWS01	4,995.95	2016	AP	2016-03-24	2016-03-24
262		PWS01	4,995.95	2016	AP	2016-03-30	2016-03-30
263		JUS01	4,995.95	2016	VISA	2016-03-30	2016-03-29
264		INF01	5,122.50	2019	VISA	2018-07-17	2018-07-16
265		INF01	5,122.50	2019	AP	2018-05-31	2018-05-25
266		ENR01	5,173.20	2018	VISA	2017-05-24	2017-05-23
267		ENR01	5,173.20	2018	AP	2017-04-19	2017-03-02
268		MAC01	5,175.41	2020	AP	2019-05-23	2019-05-16

GNWT Expense Data Analysis
7820-21-GNWT-151-139
April 1, 2016 to November 30, 2019

#	Merchant	AP_Unit	Amount	Fiscal Year	Type	Posted	Trans_Date
269	24(1)(a)(i)(B), (ii) and (iii)(B)	INF01	5,175.41	2020	VISA	2019-05-16	2019-05-14
270		ITI01	5,221.24	2017	AP	2016-07-28	2016-07-28
271		ITI01	5,221.24	2019	VISA	2018-08-20	2018-08-17
272		INF01	6,328.89	2019	VISA	2018-08-15	2018-08-14
273		INF01	6,328.89	2018	AP	2018-01-23	2018-01-12
274		JUS01	6,412.40	2018	VISA	2018-03-09	2018-03-08
275		JUS01	6,412.40	2018	AP	2018-02-28	2018-02-06
276		INF01	6,532.10	2020	VISA	2019-08-05	2019-08-02
277		INF01	6,532.10	2020	AP	2019-07-09	2019-05-29
278		INF01	7,152.63	2018	VISA	2017-10-06	2017-10-05
279		INF01	7,152.63	2018	AP	2017-09-07	2017-09-07
280		INF01	7,211.50	2019	AP	2018-07-11	2018-06-13
281		INF01	7,211.50	2019	VISA	2018-07-11	2018-07-10
282		ITI01	7,216.25	2019	AP	2018-09-17	2018-02-28
283		ITI01	7,216.25	2019	VISA	2018-09-19	2018-09-18
284		INF01	7,400.05	2020	AP	2019-08-16	2019-07-26
285		INF01	7,400.05	2020	VISA	2019-08-02	2019-08-01
286		FIN01	7,502.50	2018	VISA	2018-03-26	2018-03-22
287		FIN01	7,502.50	2018	AP	2018-03-05	2018-02-28
288		JUS01	7,609.72	2019	VISA	2018-09-17	2018-09-14
289		JUS01	7,609.72	2019	VISA	2019-01-30	2019-01-29
290		JUS01	7,609.72	2019	AP	2018-10-18	2018-10-01
291		JUS01	7,609.72	2019	AP	2018-12-17	2018-12-01
292		JUS01	7,829.72	2019	VISA	2018-09-17	2018-09-15
293		JUS01	7,829.72	2019	AP	2018-08-20	2018-08-01
294		INF01	8,105.09	2020	VISA	2019-11-04	2019-11-01
295		INF01	8,105.09	2020	AP	2019-10-24	2019-07-31
296		ENR01	8,616.87	2018	VISA	2018-02-28	2018-02-27
297		ENR01	8,616.87	2018	AP	2018-03-12	2018-02-16
298		ECE01	9,051.60	2019	VISA	2018-05-07	2018-05-04
299	ECE01	9,051.60	2019	AP	2018-06-15	2018-04-02	
300	ENR01	9,377.24	2017	VISA	2016-07-11	2016-07-08	
301	ENR01	9,377.24	2017	AP	2016-09-15	2016-07-06	
302	INF01	9,667.62	2018	VISA	2018-03-20	2018-03-19	
303	INF01	9,667.62	2018	AP	2018-02-20	2018-02-05	
		Total Amount	851,305.49				
		Total Count	303				



CONFIDENTIAL

May 18, 2021

File: 7820-20-GNWT-151-139

MR. SANDY KALGUTKAR
DEPUTY MINISTER
FINANCE

Audit Report: Expense Data Analysis, Phase IV: Timing of Payments
Audit Period: April 1, 2016 to March 31, 2020

A. SCOPE AND OBJECTIVES

The Audit Committee approved the data analysis of the Government of the Northwest Territories (GNWT) departmental expenditures to assess compliance with the Financial Administration Manual (FAM) directives. The audit scope was all departmental expenditure transactions processed between April 1, 2016, and November 30, 2019, that could be tested for compliance with FAM using data analysis. Due to delays in reporting caused by the COVID-19 response, additional analysis was completed up to March 31, 2020.

The audit analysis was divided into various phases, such as duplicate VISA transactions, invoicing errors, and timing of payments. This report covers issues related to the timing of payments processed through the GNWT's accounts payable process.

B. BACKGROUND

The GNWT disbursed approximately \$2 billion annually on operating and capital expenses. From April 2016 to March 2020, the GNWT processed over 428,000 accounts payable transactions totalling over \$7.7 billion. Concurrently, the GNWT processed over 412,000 Corporate Credit Card (VISA) transactions totalling over \$176 million.

Financial Employee Shared Services (FESS) was responsible for processing payments for GNWT departments through the System for Accountability and Management (SAM) Accounts Payable (AP) module. FESS was expected to process AP payments over \$10,000, while payments under \$10,000 were usually processed by departments using VISA. Vendors were to send their invoices directly to FESS for payment. FESS required the department's expenditure authority to verify all invoices before processing a payment in SAM.

C. OVERVIEW

The GNWT had defined different payment terms within FAM depending on the type of vendor – net 20 for vendors registered with the Business Incentive Policy (BIP) and net 30 for non-BIP vendors.

About 5.5% (904 of 16,360) of vendors in SAM were classified as BIP and accounted for 13% (\$1.0 of \$7.7 billion) of payments (**Schedule I Refers**). The top 30 vendors (0.2%) accounted for over 35% (149,528 of 426,538) of all transactions (**Appendix A Refers**). The listing showed that ten NWT public sector entities were not classified as BIP vendors. The inclusion of these ten vendors as BIP would double the BIP classified payments to \$2.1 billion, accounting for 27% of all payments.

In recent years the GNWT's entire effort to pay vendors on time had not been made public. Data analysis of over 426,000 SAM AP payments identified 78% (332,000 of 426,000) compliance with FAM 720. By including all 412,000 VISA transactions in the calculation, the FAM 720 compliance increases to 89%. (**Schedule I Refers**). FAM 720 BIP compliance could not be analyzed as the VISA file did not track BIP status.

The rate of data entering invoices and subsequent approval by the expenditure authority impacted the time taken to make payments to vendors. The time required to enter invoices data could be significantly reduced by using an electronic interface between SAM and a vendor's financial system.

An in-depth examination of roughly 160,000 SAM AP transactions between January 2018 and March 2020 showed that:

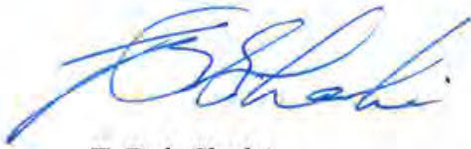
- 50% of invoices were data entered and approved by a department expenditure authority within the first ten days of receipt of the invoice.
- 84% of invoices moved from expenditure authority through accounting authority to payment within the last ten days of the AP process (**Schedule II Refers**).

Additional analysis of the DIIMS workflow used by FESS would be required to determine the root cause of the bottleneck in payment processing.

The Office of the Comptroller General agreed to a management action plan to improve internal controls and mitigate the identified risks.

D. ACKNOWLEDGEMENT

We want to thank the Department of Finance Reporting, Treasury & Risk Management Division's Financial Reporting section and the SAM team for their assistance and co-operation throughout this phase of the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Observation 1: GNWT Payment Terms

Criteria
<p>Financial Administration Manual (FAM) 720 – Timing of Payments: Payment must be made within 20 days to Business Incentive Policy (BIP) registered vendors and within 30 days for non-BIP vendors by the latter of the (1) invoice date, (2) receipt of goods or services, (3) completion of contract terms.</p> <p>FAM 730 – Corporate Credit Cards: Corporate Credit Cards were the primary payment method for purchases of goods and services up to \$10,000.</p> <p>FAM 725 – Interest on Late Payments to Vendors: Interest resulting from late payment shall only be paid... when a contract is in place that specifically provides for payment of interest or a payment has been unreasonably delayed over 61 days after the invoice date.</p>
Condition / Evidence
<p>The GNWT used two processes to pay vendors invoices:</p> <ul style="list-style-type: none">• System for Accountability and Management accounts payable module (SAM AP)• Corporate Credit Cards (VISA) <p>SAM AP payments between April 1, 2016 and March 31, 2020, totaling \$7.7 billion were:</p> <ul style="list-style-type: none">• 87% for non-BIP vendors (15,459 of 16,363) accounted for \$6.7 billion of payments• 13% for BIP vendors (904 of 16,363) accounted for \$1.0 billion of payments. <p>The 30 highest volume vendors accounted for over 35% of all transactions (149,528 of 426,538). We noted that from the 18 of those 30 non-BIP vendors, ten vendors were public sector entities. BIP classified spending would increase to \$2.1 billion (27%) if those ten vendors were classified as BIP vendors (Appendix A refers).</p> <p>SAM AP used “Basis Date” to identify the latter of the invoice date, the date the invoice was received by GNWT or the date the contract terms were completed. SAM AP data analysis of 426,538 transactions showed that:</p> <ul style="list-style-type: none">• 78% (332,013 of 426,538) of transactions complied with FAM 720. The level of compliance was:<ul style="list-style-type: none">○ 68% for BIP vendor transactions (103,267 of 152,531)○ 84% for non-BIP vendor transactions (228,746 of 274,007).• 6% of the transaction were paid more than 60 days after the due date. The delay for the two types of vendors was:<ul style="list-style-type: none">○ 4% for BIP vendor transactions (5,876 of 152,531)○ 7% for non-BIP vendor transactions (19,196 of 274,007).

**Department of Finance
GNWT Expense Data Analysis
7820-20-GNWT-151-139**

In September 2001, GNWT began using corporate credit cards to make payments to local vendors in place of the Local Contract Authority (LCA, FAM 3304). This change reduced the time and effort required to process payments, and vendors benefited by receiving immediate payment for the sale of goods and services. For the data analysis period, approximately 412,000 VISA transactions totalling \$176 million were processed by GNWT. The payment-to-vendor compliance with FAM 720 increased from 78% to 89% once the VISA transactions were considered in conjunction with SAM AP payments. Compliance with BIP and non-BIP requirements could not be assessed as VISA did not track BIP status.

Risk/Consequence	
<ul style="list-style-type: none"> • Non-conformance with FAM 720 may have resulted in: <ul style="list-style-type: none"> • Late payments, which may be detrimental to vendors or cause reputational damage to the GNWT. • Potential interest penalties on late payments to vendors. • The full effort by GNWT to support northern businesses may not be captured as public sector entities are considered non-BIP. • The full effort by GNWT to pay vendors on time may not be captured as VISA payments were omitted when reporting conformance with FAM 720. 	<p>Risk Rating: Medium Likelihood: Likely Impact: Moderate Risk Owner: Comptroller General, Finance Support: Executive Director, FESS - FIN Executive Director, ERP - FIN Director, Finance & Administration - ITI</p>
Recommendations	
<p>We recommend the Comptroller General:</p> <ol style="list-style-type: none"> 1. Include VISA payments when reporting overall statistics for the timing of payments. 2. Work with SAM Team and ITI to review and update public sector entities to be included in BIP reporting. 3. Support development of a strategy to increase BIP vendor participation. 4. Work with SAM Team and VISA to identify and track BIP versus non-BIP VISA vendors. 	
Suggested Management Response	Timeline
<p>The Comptroller General will:</p> <ol style="list-style-type: none"> 1. Include payments to vendors through the SAM AP module when reporting timeliness of payments (20 and 30 days). FESS is designing the reporting framework for this as there are a number of considerations for example contribution agreements and utilities. 2. Using the reporting information in item 1, analyze the data to determine trends and potential areas for additional training etc. to increase the number of invoices paid on time. This includes engagement with the DFA community. 	<p>August 2021</p> <p>December 2021</p>

Observation 2: Timeliness of Payment Processing

Criteria
<p>Financial Administration Manual (FAM) 720 – Timing of Payments: Payment must be made within 20 days to Business Incentive Policy (BIP) registered vendors and within 30 days for non-BIP vendors by the latter of the (1) invoice date, (2) receipt of goods or services, (3) completion of contract terms.</p> <p>Financial Employee Shared Services (FESS) Business Process - Basis Date must be entered as the date the invoice was received or the date the goods/services were received (or construction completed), whichever was latest. The Basis Date and Pay Terms (Immediate, Net 20, and Net 30) drove the Scheduled Due Date (Payment Date).</p>
Condition / Evidence
<p>Data entry of invoices was labour intensive and time-consuming. SAM could reduce data entry by utilizing an electronic interface. We noted that:</p> <ul style="list-style-type: none"> • 0.2% of all vendors (30 of 16,360) made up over one-third of total transactions (149,528 of 426,538). • Over 24% of payments to these 30 vendors were paid outside of conformance with FAM 720 (Appendix A Refers). <p>We conducted in-depth data analysis of the key stages in processing AP invoices for almost 160,000 transactions processed between January 2018 and April 2020. When considering five business days for each stage, the data analysis showed:</p> <div style="text-align: center; margin: 10px 0;"> <pre> graph LR A[Basis Date] -- 46% --> B[Entered Date (invoice data entered)] B -- 53% --> C[Expenditure Approval Date] C -- 89% --> D[Accounting Approval Date] D -- 78% --> E[Payment Date] </pre> </div> <ul style="list-style-type: none"> • FESS used SAM and a DIIMS workflow to communicate and review invoices with departments. An assessment of the DIIMS workflow was outside the scope of our data analysis. • SAM did not provide notification to the Expenditure Officer when an invoice was ready for approval. A reminder email was sent each Saturday if transactions were outstanding for more than two days. <p>Additional analysis would be required to determine the cause of the bottleneck between the basis date and expenditure approval.</p>

Department of Finance
GNWT Expense Data Analysis
7820-20-GNWT-151-139

Risk/Consequence	
<ul style="list-style-type: none"> • A labour-intensive payment process may be time-consuming, use valuable resources, or decrease payment accuracy. • The rate of data entering invoices and approval by departments impacts the length of time taken to make payments. Delays may: <ul style="list-style-type: none"> • Be detrimental to vendors. • Cause reputational damage to the GNWT. 	<p>Risk Rating: Medium Likelihood: Likely Impact: Moderate Risk Owner: Comptroller General, Finance Support: Executive Director, ERP – FIN Executive Director, FESS – FIN DFA Community</p>
Recommendations	
<p>We recommend the Comptroller General:</p> <ol style="list-style-type: none"> 1. Engage FESS and SAM to develop a protocol to engage vendors with large volumes of invoices and utilize an electronic interface. 2. Engage FESS and the DFA community to conduct further analysis of the SAM and DIIMS processes between the basis date and the expenditure approval to determine the root cause of the bottleneck in payment processing, and subsequently, if the issue(s) can be resolved. 	
Suggested Management Response	Timeline
<p>The Comptroller General will review current processes for financial processing to see if any efficiencies can be made.</p>	<p>December 2021</p>

Department of Finance
GNWT Expense Data Analysis
7820-30-GNWT-151-139
April 1, 2016 to March 30, 2020

Appendix A

Top 30 Vendors by Transaction

Vendor Name	Supplier ID	BIP (Note 1)	Transactions		Late (Note 2)	
			Number	Percentage	Number	Percentage
24(1)(a)(i)(B), (ii) and (iii)(B)		Yes	40,118	9.4%	4,450	11.1%
		No*	25,233	5.9%	778	3.1%
		No*	11,155	2.6%	1,686	15.1%
		No	5,488	1.3%	439	8.0%
		No	4,312	1.0%	1,106	25.6%
		No*	4,057	1.0%	694	17.1%
		Yes	3,712	0.9%	966	26.0%
		No*	3,594	0.8%	820	22.8%
		No	3,498	0.8%	81	2.3%
		No*	3,347	0.8%	1,708	51.0%
		Yes	3,325	0.8%	1,464	44.0%
		Yes	3,131	0.7%	819	26.2%
		Yes	2,949	0.7%	447	15.2%
		Yes	2,810	0.7%	861	30.6%
		Yes	2,772	0.6%	940	33.9%
		No*	2,757	0.6%	1,724	62.5%
		No	2,559	0.6%	490	19.1%
		No	2,538	0.6%	804	31.7%
		Yes	2,409	0.6%	810	33.6%
		No	2,066	0.5%	176	8.5%
		No*	1,957	0.5%	415	21.2%
		No*	1,913	0.4%	5	0.3%
		Yes	1,867	0.4%	604	32.4%
		No*	1,864	0.4%	238	12.8%
		Yes	1,846	0.4%	515	27.9%
		No*	1,819	0.4%	285	15.7%
		No	1,670	0.4%	708	42.4%
		No	1,662	0.4%	249	15.0%
		Yes	1,576	0.4%	771	48.9%
		Yes	1,524	0.4%	524	34.4%

Notes:

1. Public sector entities not classified as BIP (*).
2. "Late":
 - a. BIP-Registered vendors - payments made 20 days after Basis Date
 - b. Non-BIP vendors - payments made 30 days after Basis Date.



CONFIDENTIAL

November 29, 2021

File: 7820-20-GNWT-151-139

MR. WILLIAM MACKAY
DEPUTY MINISTER
FINANCE

Audit Report: Expense Data Analysis, Phase V: Contract Splitting Using Visa
Audit Period: April 1, 2020 to March 31, 2021

A. SCOPE AND OBJECTIVES

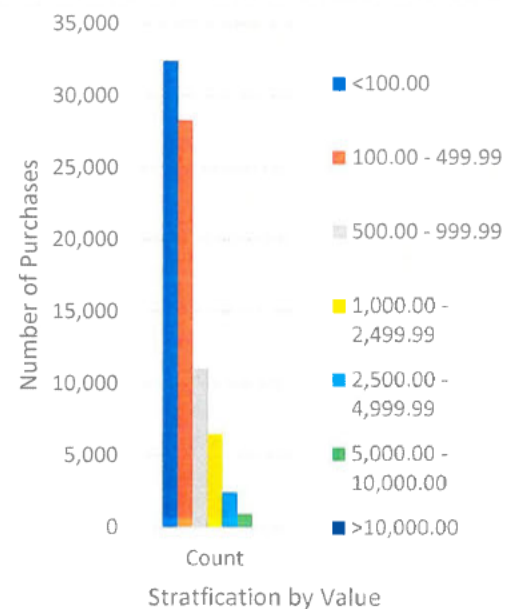
The Audit Committee approved the data analysis of the Government of the Northwest Territories (GNWT) departmental expenditures to assess compliance with the Financial Administration Manual (FAM) directives. The project was divided into multiple phases among which were duplicate payments, timing of payments, and contract splitting. For this phase, we focused our analysis of credit card (Visa) payments from April 1, 2020 to March 31, 2021 identifying potential contract splitting.

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

B. BACKGROUND

Since September 2001, GNWT has used Visa to pay for small purchases. Over 1,600 cardholders used their Visa to pay for goods and services. While this accounted for about 2% (\$40 million of \$2 billion) paid by GNWT, it accounted for nearly half the payments (81,480 of 172,009). As illustrated in the chart, majority of the transactions were for under \$500.

The Visa cardholders were to follow FAM, Visa One Manual, and the GNWT Procurement Procedures Manual.



C. OVERVIEW

The GNWT procurement frameworks expected the contracting authorities (i.e., Visa users) to conduct procurement in manner that will withstand public scrutiny in matters of integrity, fair competition, transparency, and accountable management of public funds and resources that provides value to NWT residents.

Purchase of items under \$10,000 had been decentralized to departments while departments engaged Procurement Shared Services (PSS) to handle larger and more complex procurement. Transactions could be split to avoid PSS oversight and the procurement competitive requirements.

Most Visa transaction were processed in compliance with procurement guidelines. Using data analysis, and subsequent confirmation by three departments, we identified a very small sample of transactions that had been split (**Schedule I refers**). Data analysis narrowed down the high-risk transaction and subsequent manual review identified 113 high-risk transactions. Sample testing of these high-risk transactions for three departments showed that 34% (15 of 43) were split.

Splitting of transaction to avoid government procurement guidance damaged the procurement community reputation of PSS and throughout the GNWT. The PSS Quality Assurance process could leverage data analytics or relevant automated tools to identify and monitor the complete procurement universe.

D. ACKNOWLEDGEMENT

We want to thank the Departments of Finance, Executive and Indigenous Affairs, and Environment and Natural Resources for their assistance and cooperation throughout this audit phase.



Stephanie Carter
Director, Internal Audit Bureau
Finance

**Department of Finance
GNWT Expense Data Analysis
7820-30-GNWT-151-139**

SCHEDULE I

Observation: Phase V – Contract Splitting using Visa Payments

Criteria	
<p>GNWT Procurement Procedures Manual:</p> <ul style="list-style-type: none"> • Subsection 1.7.1 – Services procurement of more than \$10,000 required two (2) written quotes • Subsection 1.7.1.3 – To demonstrate that the best value was obtained for the GNWT, it was recommended that departments get two (2) written quotes for all purchases under \$25,000. 	
Condition / Evidence	
<p>Departments spent over \$40 million using visas from April 1, 2020 to March 31, 2021, processing over 81,000 transactions. Data analysis showed that nearly 3% (2,330 of 81,480) of the transactions over \$1,000 were paid by the cardholders to the same vendor multiple times on a given day and charged to the same general ledger account in the financial system for the same department activity. These transactions were all reviewed and approved by the spending authority of the departmental activity.</p> <p>The examination of over 2,300 matching transactions identified 370 transactions where contracts splitting may have occurred to avoid procurement guidelines. An in-depth examination indicated that 113 of the 370 transactions were highly likely to be non-compliant. Three departments were asked to provide the supporting documents for 43 transactions (Schedule II refers). The analysis shows that 35% (15 of 43) transactions did not comply with procurement guidelines as follows:</p> <ul style="list-style-type: none"> • Executive and Indigenous Affairs was fully compliant • Energy and Natural Resources at 44% (8 of 18) • Finance at 31% (7 of 22). 	
Risk / Consequence	
<p>Cardholders making VISA purchase by asking vendors to split payment to avoid procurement guidelines could damage GNWT's procurement community reputation.</p>	<p>Risk Rating: Medium Likelihood: Almost Certain Impact: Minor Risk Owner: Comptroller General Support:</p> <ul style="list-style-type: none"> • Director, Procurement Shared Services (PSS), FIN • Manager, Quality Assurance, PSS, FIN
Recommendation	
<p>The appropriate Division within Finance will implement a data analytics process to identify contract splitting in Visa transactions. This process would include annual reports to the Procurement Procedures Committee.</p>	
Management Response:	Timeline:
<ul style="list-style-type: none"> • The department will review the recommendations to determine which division within the department Finance should be responsible to implement process that will include using data analytics to identify contract splitting using visa cards and annually report the results to the Procurement Procedures Committee. • PSS will continue to educate department on how to procure goods and services under the thresholds and review and update the procurement guidelines 	<p>May 2022 to implement the process of using the data analytics.</p>

ENR VISA Transactions

CARDHOLDER NAME	MERCHANT	TRANSACTION DATE	AMOUNT	DEPTID	GL ACCOUNT	PROGRAM CODE	Split	False Positives
23(2)(d)	NORTHERN FANCY MEATS	10/23/2020	\$ 17(1)	53019	53150	55062	\$ 17(1)	
	NORTHERN FANCY MEATS	12/18/2020	17(1)	53019	53150	55062	\$	
	NORTHERN FANCY MEATS	12/18/2020	17(1)	53019	53150	55062		
	YELLOWKNIFE MOTORS	1/4/2021		53038	53150	55197		17(1)
	YELLOWKNIFE MOTORS	1/4/2021		53038	53150	55197		
	PACIFIC SAFETY PRODUCT	11/25/2020		53005	53150	55016	17(1)	
	PACIFIC SAFETY PRODUCT	11/25/2020		53005	53150	55016		
	PACIFIC SAFETY PRODUCT	11/25/2020		53005	53150	55016		
	736 EMCO YELLOWKNIFE	11/24/2020		53039	53180	55198		17(1)
	736 EMCO YELLOWKNIFE	11/24/2020		53039	53180	55198		
	736 EMCO YELLOWKNIFE	11/24/2020		53039	53180	55198		
	736 EMCO YELLOWKNIFE	11/24/2020		53039	53180	55198		
	WAVE - *DRW ANDASSOCIATES	3/8/2021		53030	53450	55051	17(1)	
	WAVE - *DRW ANDASSOCIATES	3/8/2021		53030	53450	55051		
	GLOBAL LAB SUPPLY	12/18/2020		49027	53560	25105		17(1)
	GLOBAL LAB SUPPLY	12/18/2020		49027	53560	25105		
	INVITROGEN-CANADA	7/8/2020		53039	53150	55198		
	INVITROGEN-CANADA	7/8/2020		53039	53150	55198		
Total Amount			\$ 104,820.49				\$ 53,530.71	\$ 51,289.78
Total Count			18				8	10

EXE VISA Transactions

CARDHOLDER NAME	MERCHANT	TRANSACTION DATE	AMOUNT	DEPTID	GL ACCOUNT	PROGRAM CODE	Split	False Positives
23 (2)(d)	IN *ARTLESS COLLECTIVE IN	4/30/2020	17(1)	11030	53070	10001	-	\$ 17(1)
	IN *ARTLESS COLLECTIVE IN	4/30/2020		11030	53070	10001	-	
	IN *ARTLESS COLLECTIVE IN	4/30/2020	17(1)	11030	53070	10001	-	
Total Amount			\$ 12,728.02				-	\$ 12,728.02
Total Count			3				-	3

FIN VISA Transactions

CARDHOLDER NAME	MERCHANT	TRANSACTION DATE	AMOUNT	DEPTID	GL ACCOUNT	PROGRAM _CODE	Split	False Positive
23(2)(d)	CREATIVE BASICS	4/20/2020	17(1)	15001	53740	0	\$ 17(1)	
	CREATIVE BASICS	4/20/2020	17(1)	15001	53740	0		
	RRU STUDENT	2/19/2021		15045	50322	20040		17(1)
	RRU STUDENT	2/19/2021		15045	50322	20040		
	NORTHERN TRANSITION	9/11/2020		21070	53120	25105		
	NORTHERN TRANSITION	9/11/2020		21070	53120	25105		
	YELLOWKNIFE	7/20/2020		21070	53030	25105		
	YELLOWKNIFE	7/20/2020		21070	53030	25105		
	YELLOWKNIFE	7/9/2020		53039	53250	25105		
	YELLOWKNIFE	7/9/2020		53039	53250	25105		
	HERITAGE HOTEL	11/2/2020		15004	50230	0	17(1)	
	HERITAGE HOTEL	11/2/2020		15004	50230	0		
	HERITAGE HOTEL	11/2/2020		15004	50230	0		
	BEST MOVERS	9/9/2020		15003	13085	25061		17(1)
	BEST MOVERS	9/9/2020		15003	13085	25061		
	BEST MOVERS	9/9/2020		15003	13085	25061		
	LAC LA MARTE DEVELOPMENT	10/5/2020		15002	13085	25062	17(1)	
	LAC LA MARTE DEVELOPMENT	10/5/2020		15002	13085	25062		
	BEST MOVERS	8/20/2020		15002	13085	25048		17(1)
	BEST MOVERS	8/20/2020		15002	13085	25048		
BEST MOVERS	10/13/2020		15002	13085	25052			
BEST MOVERS	10/13/2020		15002	13085	25048			
Total Amount			\$ 133,043.07				\$ 33,482.07	\$ 99,561.00
Total Count			22				7	15



MAY 31 2018

CONFIDENTIAL

File: 7820-30-GNWT-151-114

MR. DAVID STEWART
CHAIR, INFORMATICS POLICY COUNCIL
FINANCE

Audit of GNWT Cyber Security Resilience Report

Enclosed is the above referenced Audit Report.

The Internal Audit Bureau will schedule a future follow-up audit. However, in the interim, we would like to be notified of any progress in implementing the changes to regulations, policy, or practices by November 30, 2018.

Should you have any questions concerning the Audit Report, 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
Mr. Dave Heffernan, Chief Information Officer, Finance



Audit of GNWT Cyber Security Resilience

GNWT-WIDE Information Technology Audit Report

Internal Audit Bureau

May 2018



Audit Report Information Technology Audit

AUDIT OF GNWT CYBER SECURITY RESILIENCE

May 2018

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



CONFIDENTIAL

May 31, 2018

File: 7820-30-GNWT-151-114

MR. DAVID STEWART
CHAIR, INFORMATICS POLICY COUNCIL
FINANCE

Audit Report: Audit of GNWT Cyber Security Resilience
Audit Period: November 1, 2017 to March 31, 2018

A. SCOPE AND OBJECTIVES

The Audit Committee approved the Cyber Security Resilience audit to assess the internal controls set in place by the Informatics Policy Council (IPC).

B. BACKGROUND

Section 7 of the *Financial Administration Act (FAA)* assigns the Financial Management Board (FMB) the responsibility for plans, policies and strategies associated with information management and technology. The IPC establishes the policy framework for Information Communication and Technology (ICT) with the support from the Office of the Chief Information Officer (OCIO).

The OCIO works with all stakeholders in all aspects of its mandate to ensure that ICT investments, assets, and operations support the business goals of the GNWT in an effective, efficient and economical manner. As well, the OCIO provides day-to-day guidance to all stakeholders regarding ICT strategy, security and policy implementation.

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

The network maintained by the Technology Service Center (TSC), Department of Infrastructure, supports nearly 200 applications throughout the GNWT.

Grant Thornton was awarded a contract through the competitive Request for Proposals process that was evaluated by a team composed of staff from OCIO and Internal Audit Bureau (IAB).

C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached report by Grant Thornton “*IT Audit – Cyber Security Resilience*” (**Appendix A refers**) made a number of observations pertaining to the audit objective. Some of the positive observations were:

- 1) There was breadth and depth of policies, standards, and guidance.
- 2) Application Inventory was maintained by the OCIO.
- 3) Vulnerability Assessment has been done on newly introduced or upgraded applications.
- 4) OCIO has taken steps to improve security awareness by implementing an on-line security awareness training program.

20(1)(k)

Some of the specific messages from the audit report were:

- 1) 20(1)(k)
- 2)
- 3)
- 4)
- 5)
- 6)

20(1)(k)

20(1)(k)

The IAB will follow-up on the status of the management action plan for the next fiscal year during our scheduled follow-up audits.

The audit work for this phase of Cyber Security focused on two areas: Identify and Protect. The assessment of other three areas (Detect, Respond, and Recovery) should be undertaken soon for a complete coverage of Cyber Security risk.

D. ACKNOWLEDGEMENT

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

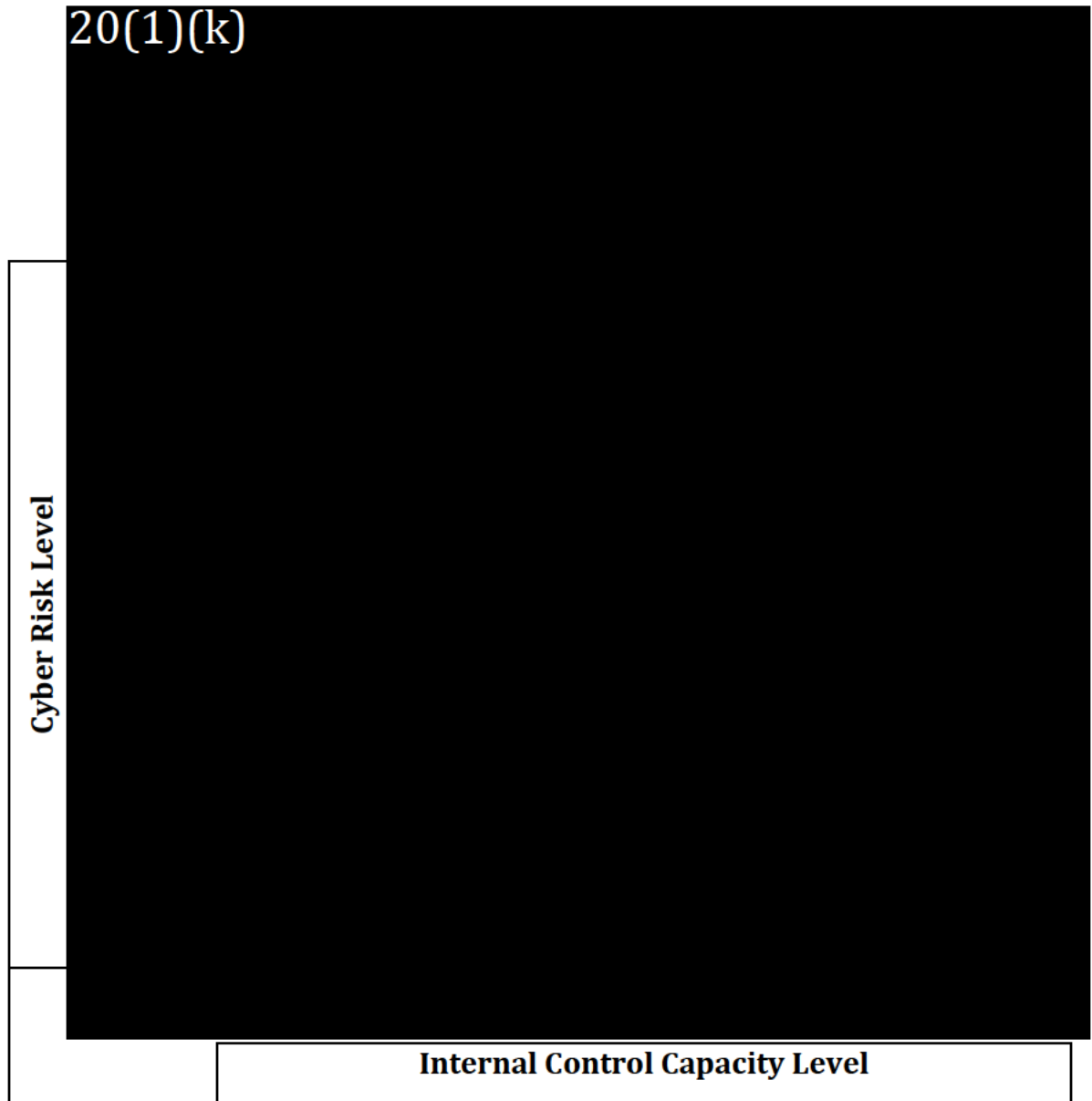


T. Bob Shahi
Director, Internal Audit Bureau
Finance

7820-30-GNWT-151-114
Audit of GNWT Cyber Security Resilience
November 1, 2017 to March 31, 2018

Risk and Opportunity Assessment Using Capacity Model

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



Risk Level and Internal Control Capacity Level are Matched.

Government of the Northwest Territories

Audit Report



IT Audit – Cyber Security Resilience

March 2018

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY	3
1.1 Background / Context.....	3
1.2 Audit Objectives and Scope	3
1.3 Summary of Observations and Recommendations	4
1.4 Audit Methodology	6
2.0 DETAILED FINDINGS.....	7
APPENDIX A – AUDIT CRITERIA	20
APPENDIX B – FINDINGS RATING SCALE	22
APPENDIX C – NIST FRAMEWORK	23

1.0 EXECUTIVE SUMMARY

1.1 Background / Context

In November 2017, the Internal Audit Bureau engaged Grant Thornton LLP (GT) to conduct GNWT Cyber Resilience Audit. The Government of the Northwest Territories (GNWT) has 11 departments and 13 agencies, delivering a full range of province like services to citizens of the Northwest Territories (NWT). GNWT departments and agencies use technology and internal tools to deliver programs to NWT citizens and to support administrative and management functions. A department or agency can have a few dozen applications to meet its program needs. Currently, there are over 450 applications used throughout the GNWT. PeopleSoft is used on a corporate level, and the remaining applications vary by department or agency.

Key departments, such as Health & Social Services and their Boards, use applications containing private and confidential information to deliver vital health related programs and services in the NWT. Some other departments are depicted in the table below:

Department	Program/Service
Infrastructure (INF)	Transportation
Environment & Natural Resources (ENR)	Air Quality and Fire
Education, Culture & Employment & Boards (ECE)	Income & Education Programs
Municipal and Community Affairs (MACA)	Community Service Programs
Justice	Corrections & Courts Services

20(1)(k)

1.2 Audit Objectives and Scope

The objective of this audit is to assess internal controls set in place by the Informatics Policy Council in addressing cyber security threats using NIST framework and focusing on Identify and Protect functions.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. **Please see Appendix C for more details on the NIST Framework.** It provides methodologies to assess and manage cyber security related risks more proactively. It is useful in the context of GNWT, since it is considered as a best practice for cyber security and includes five functions or categories (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover. The reason why only the first two categories were included is because they are fundamental, yet important elements to identify and protect assets, information, systems and so on from cyber security risks. These processes and controls therein are more preventative in nature and more proactive, therefore, they are the starting point used for this audit.

Our audit scope covered the following departments, and corresponding selected applications operated by them:

In-Scope Departments of North West Territories	In-Scope Applications
Finance	System for Accountability and Management (SAM)
Health and Social Services	Electronic Medical Records (EMR)
Infrastructure	Active Directory, Digital Integrated Information Management

Our site visits occurred in one (1) region – Yellowknife.

1.3 Summary of Observations and Recommendations

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

The following positive observations were identified through the audit:

- The auditors are satisfied with the breadth and depth of the security policies, standards and guidance documents including acceptable use policies, internet use policy, records management and disposal policies, and assertions made within such documents to the requirement to meeting jurisdictional obligations, requirement for compliance, and to manage user expectations to privacy when using GNWT information assets.
- While GNWT did not meet audit criteria for Asset Management, there is an evidence demonstrating awareness of the objective to manage assets to the extent that enables the government to respond to incidents affecting application security, privacy and technical support requirement. This was evidenced by the OCIO’s attempts to maintain a comprehensive Application Inventory.

20(1)(k)

- There is demonstrable evidence showing that the OCIO has taken steps to improve security awareness including the implementation of an on-line security awareness training program and relevant awareness posters.

The table below classifies and prioritizes the key findings for each audit Area according to the impact on the organization (as defined in Appendix B – Findings Rating Scale).

Audit Area	Key Observations	Impact	Report
------------	------------------	--------	--------

		Assessment	Section
1. Policies and procedures	■	20(1)(k)	2.1
2. Policies and procedures	■		2.1
3. IT Risk Management and Vulnerability Assessments	■		2.2
4. Incident handling and response	■		2.3
5. Enterprise Network and Security Architecture	■		2.4
6. IT Asset Management Strategy	■		2.5
7. Security Awareness Training	■		2.6
8. Other identified issues and concerns	■		2.7
9. Other identified issues and concerns	■		2.7

1.4 Audit Methodology

The audit was conducted in a manner consistent with *Internal Auditing Standards* and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

The audit examined relevant evidence and obtain sufficient information to provide a reasonable level of assurance in support of the audit conclusion.

During the planning phase, the following key audit activities were completed:

- Project planning;
- Document collection and review;
- Stakeholder interviews;
- Process walkthrough;
- Summarizing risks/business issues, identifying lines of inquiry and audit criteria;
- Preparing audit tools and templates (audit program, templates, interview guides); and
- The Audit Plan was sent to IAB for approval.

During the conduct phase, the following key audit activities were completed:

- Completing the audit program including testing the identified controls;
- Documenting interviews conducted through meeting minutes;
- Documenting process walkthroughs;
- Completing working papers and preparing lead sheets;
- Reporting any significant findings throughout the course of this audit to the appropriate management level as they are discovered; and
- Debriefing the auditee on audit findings.

During the reporting phase, the following key audit activities were completed:

- Preparing the draft audit report, including cause based recommendations;
- Presentation and validation of the draft audit findings with IAB and senior management; and
- Producing the final audit report and recommendations including management action plans approved by operational management.

2.0 DETAILED FINDINGS

2.1 Policies and Procedures

The auditors expected to find that GNWT has established policies that are pertinent to the security of IT assets (such as acceptable use policies, security awareness, email and expectations of privacy). We further expected to see that policies are aligned to GNWT's business objective and risk management strategies. Operationally, we expected to find that policies are operationalized and expressed in supporting documented processes and procedures and that they are being enforced throughout the organization.

Additional guidance in these areas can be found in COBIT 5: APO01, APO02, APO03, APO08, APO10, APO12, APO13, BAI02, BAI04, BAI09, DSS04, DSS05, DSS06, EDM01, MEA03 and NIST: Identify: ID. AM and ID. BE.

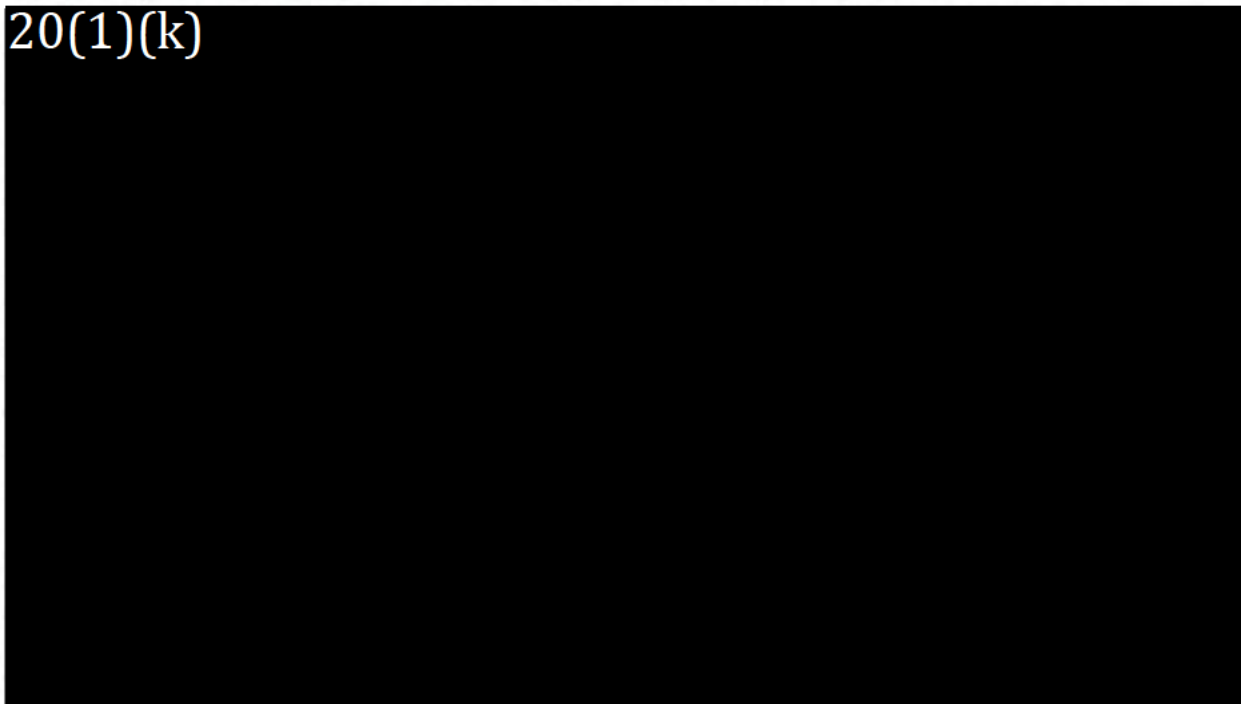
Findings

Polices exist, although, there are opportunities for improvement. The auditors are satisfied with the breadth and depth of the security policies, standards and guidance documents including acceptable use policies, internet use policy, records management and disposal policies, and assertions made within such documents to the requirement to meeting jurisdictional obligations, requirement for compliance, and to manage user expectations to privacy when using GNWT information assets.

The Informatics Policy Council (IPC) identifies the Office of the Chief Information Officer as the senior decision-making body for Information Management/Information Systems/Information Technology (IM/IS/IT) strategy and policy. The OCIO supports the IPC and acts on its behalf on day-to-day operations ensuring that policies are being followed and complied to.

Further, an Electronic Information Security Policy identifies governance committees along with applicable terms of reference to which information security-related concerns and issues are relegated for assessment, advice and resolution. That is in addition to identifying, managing and mitigating risks that are pertinent to cybersecurity, including assignment of roles and responsibilities for cybersecurity.

20(1)(k)



20(1)(k)

Impact

- 20(1)(k)

Recommendation #1

- 20(1)(k)

Recommendation #2

- 20(1)(k)

Management Responses:

Action Plan	Completion Date
Agree with recommendation #1 20(1)(k)	Fall 2020

20(1)(k)

20(1)(k)

Impact: 20(1)(k)
20(1)(k)

Recommendation 3: 20(1)(k)
20(1)(k)

20(1)(k)

Management Response:

Action Plan	Completion Date
Agree in principle with recommendation #3 20(1)(k)	A1 – Spring 2019

20(1)(k)

2.3 Incident Response Program

We expected to find a policy on and associated processes and tools for implementing an incident response program. The policy should set the tone for requirement for the program and establish terms of reference along with identifying and assigning roles and responsibilities for respective members of the incident response team, including the OCIO and departmental incident handlers. The incident handling and response process should provide details on what constitutes a breach, when and how to respond to incidents including the details of a phase approach to handling and responding along with mechanisms and tools for response and successful recovery.

Additional guidance in these areas can be found in COBIT 5: APO01, APO02, APO03, APO08, APO10, APO12, APO13, BAI02, BAI04, BAI09, DSS04, DSS05, DSS06, EDM01, MEA03 and NIST: Identify: ID. AM and ID. BE.

Findings

On a positive note, IPC issued a directive for establishing incident handling and response program. It was dated January 1, 2015. It provides direction for reporting, managing, investigating and applying lessons learned for information security incidents. It also outlines the following requirements:

- That Deputy Ministers are mandated to appoint incident handlers;
- Incidents must be investigated by *trained* incident handlers;
- Assigns roles and responsibilities for the handlers, and for the OCIO; and
- Mandates Incidents must be reported quarterly to IPC.

20(1)(k)

20(1)(k)

Impact

20(1)(k)

Recommendation #4

20(1)(k)

Management Response to Recommendation #4:

Action Plan	Completion Date
Agree with recommendation #4 20(1)(k)	A1 – Fall 2018 A2 – Spring 2019 A3 – Spring 2020

2.4 Enterprise Network and Security Architecture/Framework

We expected to find that GNWT maintains an officially adopted Enterprise Network and Security Architecture (ENSA). The goal of enterprise architecture is to create an integrated IT environment (standardized hardware and software systems) across GNWT departments, and agencies; including all of the programs and services that the government operates and instigates while assuring a tight alignment and links to the government's business objectives, public service strategy and budgetary constraints. It also, among other things, outlines requirements for meeting requirements for obtaining the Authority to Operate from a central authority (such as OCIO).

Additional guidance in these areas can be found in COBIT 5: APO01, APO07, APO13, APO11, BAI02, BAI06, BAI07, BAI09, BAI10, DSS01, DSS04, DSS05, DSS06, and NIST: Protect PR.AC, PR.DS, PR.MA, and PR.IP

Findings

20(1)(k)

■ 20(1)(k)

■

20(1)(k)

Impact: 20(1)(k)

20(1)(k)

Recommendation #5:

20(1)(k)

20(1)(k)

1. **20(1)(k)**
- 2.
- 3.
- 4.
- 5.

Management Response:

Action Plan	Completion Date
Agree with recommendation #5	A1 – Fall 2018
20(1)(k)	A2 – Spring 2020

2.5 IT Asset Management Strategy

We expected to find official IT asset management-related policies in support of an overarching strategy to manage IT assets within GNWT. We also expected to find processes and tools in place for implementing asset management practices in support of established policies and documented strategy.

IT asset management is constituted of the set of business practices that integrate financial, contractual and inventory functions to support strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment.

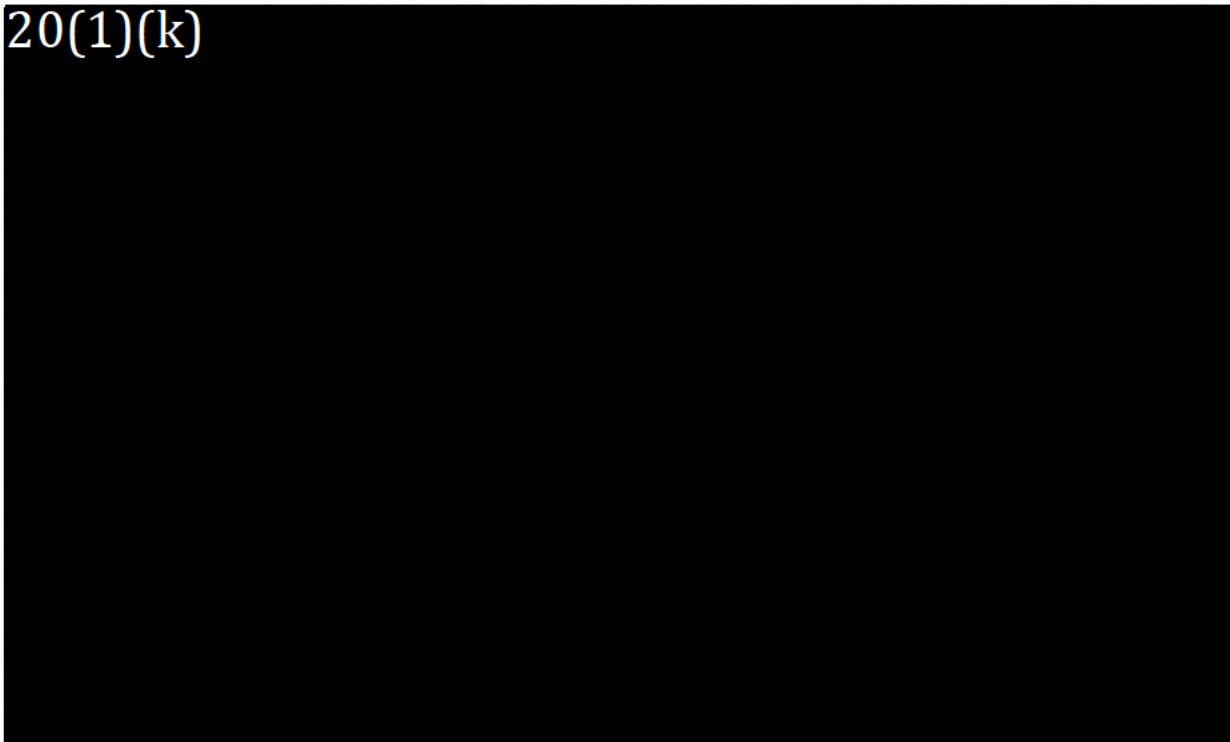
Additional guidance in these areas can be found in COBIT 5: APO01, APO02, APO03, APO08, APO10, APO12, APO13, BAI02, BAI04, BAI09, DSS04, DSS05, DSS06, EDM01, MEA03 and NIST: Identify: ID. AM and ID. BE

Findings

On a positive note, GNWT has official policies that are required for supporting asset management strategy and associated processes. Policies for identifying roles and responsibilities for the entire workforce are in place including supporting organizational charts and job descriptions.

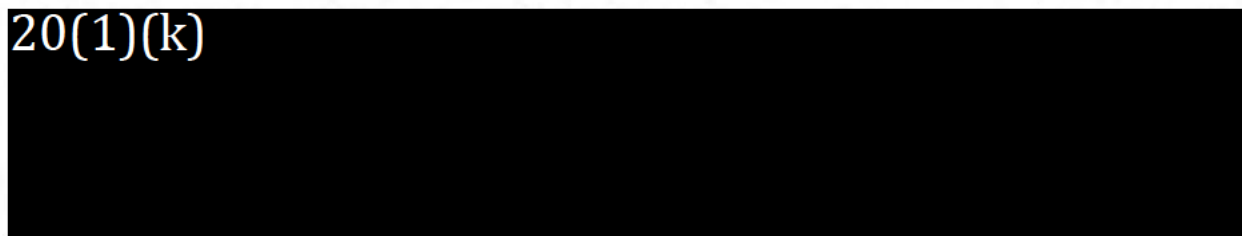
Also, GNWT maintains governance bodies along with applicable representation and terms of reference including Business Advisory Committee (BAC), Information System Advisory Committee (ISAC). Both committees report to Informatics Policy Council (IPC) which oversees initiating and approving IT-related policies including security policies.

20(1)(k)



Impact

20(1)(k)



20(1)(k)

Recommendation #6

20(1)(k)

Management Response:

Action Plan	Completion Date
Agree with recommendation #6	A1 – Spring 2020
20(1)(k)	A2 – Fall 2020
20(1)(k)	A3 – Fall 2020
20(1)(k)	A4 – Spring 2021

2.6 Security Awareness Training

We expected to find institutionalized security awareness and training program and an associated suite of processes to actively mandating GNWT employees to partake in the program offerings for increased awareness of security and risk associated with non-compliance with prevailing policies.

Additional guidance in these areas can be found in COBIT 5: COBIT: APO07, APO10, BAI05, DSS06 and NIST: Protect PR.AT

Findings

The auditors noted that GNWT deployed an online training system in July, 2017. The auditors are satisfied

with the comprehensive coverage that the security training system provides.

20(1)(k)

Impact

20(1)(k)

Recommendation #7

20(1)(k)

Management Response:

Action Plan	Completion Date
Agree with recommendation #7	Summer 2017
20(1)(k)	

2.7 Other Identified Issues and Concerns

Findings

1. 20(1)(k)

20(1)(k)

Impact: 20(1)(k)
20(1)

Recommendation 8: 20(1)(k)
20(1)(k)

Management Response:

Action Plan	Completion Date
<p>Agree in principle with recommendation #8</p> <p>20(1)(k)</p>	<p>A1 – Winter 2019</p>

2. 20(1)(k)

20(1)(k)

Impact: 20(1)(k)

20(1)(k)

Recommendation 9: 20(1)(k)

20(1)(k)

Management Response:

Action Plan	Completion Date
Agree with recommendation #9 20(1)(k)	A1 – Summer 2018

APPENDIX A – AUDIT CRITERIA

Based on the risk assessment completed, planning interviews and document review, the following audit criteria were tested to support the audit objective.

Objective	Audit Criteria	NIST Reference	COBIT 5 reference
Assess whether asset management, business environment, governance, risk assessment, and risk management strategies are effectively identified.	GNWT maintains an asset management strategy including supporting processes and procedures that is aligned to its business objectives; and used to inform cybersecurity roles, responsibilities and risk management objectives. (NIST Identify ID. AM and ID. BE).	NIST: Identify: ID. AM and ID. BE	COBIT: APO01, APO02, APO03, APO08, APO10, APO12, APO13, BAI02, BAI04, BAI09, DSS04, DSS05, DSS06, EDM01, MEA03
	GNWT maintains a risk management strategy and governance and supporting processes for identifying, managing and mitigating risks that are pertinent to cybersecurity. (NIST Identify ID. GV, ID. RA, and ID.RM).	Identify: ID. GV, ID. RA, and ID.RM	COBIT: APO12, APO13, BAI02, BAI04
Assess whether protection regarding access controls, awareness and training, data security, information processes and procedures exist	GNWT maintains information protection policy and procedures and associated data access controls that are aligned with GNWT's business objectives and risk management strategy.	Protect: PR.AC, PR.DS, PR.MA, and PR.IP	COBIT: APO01, APO07, APO13, APO11, BAI02, BAI06, BAI07, BAI09, BAI10, DSS01, DSS04, DSS05, DSS06,

	<p>GNWT's personnel and partners are provided with cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities, and agreements.</p>	<p>Protect: PR.AT</p>	<p>COBIT: APO07, APO10, BAI05, DSS06</p>
--	--	-----------------------	--

APPENDIX B – FINDINGS RATING SCALE

Our findings are classified and prioritized according to the following risk-ranking methodology¹:

Risk Ranking	Description
5. Very High	<ul style="list-style-type: none"> ■ Occurrence would have extreme impacts on stakeholders at the Government of Northwest Territories and, ■ Existing controls are inadequate or non-existent, suggesting that this risk is almost certain to materialize
4. High	<ul style="list-style-type: none"> ■ Inability or significantly reduced ability to achieve expected results and organizational priorities, and ■ Existing controls are very weak, suggesting that this risk is likely to materialize
3. Moderate	<ul style="list-style-type: none"> ■ Moderate impact on ability to achieve business objectives, and ■ Existing controls are generally adequate (few significant weaknesses) suggesting that this risk is only moderately likely to materialize
2. Low	<ul style="list-style-type: none"> ■ Limited impact on ability to achieve expected results and organizational priorities, and ■ There are minor weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize
1. Very Low	<ul style="list-style-type: none"> ■ There is little to no impact on the ability to achieve expected results and organizational priorities, and ■ There are no significant weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize

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

APPENDIX C – NIST FRAMEWORK

Category	Description	Individual components within category
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	<ul style="list-style-type: none"> ■ Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy. ■ Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. ■ Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. ■ Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. ■ Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	<ul style="list-style-type: none"> ■ Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. ■ Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. ■ Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. ■ Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. ■ Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. ■ Protective Technology (PR.PT): Technical security solutions

Category	Description	Individual components within category
		<p>are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>
<p>Detect</p>	<p>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.</p>	<ul style="list-style-type: none"> ■ Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. ■ Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. ■ Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
<p>Respond</p>	<p>Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.</p>	<ul style="list-style-type: none"> ■ Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. ■ Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. ■ Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities. ■ Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. ■ Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
<p>Recover</p>	<p>Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.</p>	<ul style="list-style-type: none"> ■ Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. ■ Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities. ■ Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.



CONFIDENTIAL

January 19, 2021

File: 7820-30-GNWT-151-112

MR. SANDY KALGUTKAR
CHAIR
INFORMATICS POLICY COUNCIL

Audit Report: DIIMS Access Monitoring
Audit Period: As of November 30, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the assessment of internal controls over access to electronic records in the GNWT departments. The audit scope was the Digital Integrated Information Management System (DIIMS) used by most departments to capture and store electronic information. The audit objectives were to determine whether:

- there was an adequate governance framework to manage electronic information in DIIMS.
- information used for monitoring DIIMS access was relevant, current, complete, timely, and accurate.
- the monitoring process was in place to ensure only authorized users had access to the information in DIIMS.

B. BACKGROUND

The NWT *Financial Administration Act* (FAA) assigned the Financial Management Board (FMB) responsibility for the approval of plans, policies and strategies associated with information management and technology (IMT). The FMB established the Informatics Policy Council (IPC) to oversee the IMT in the GNWT. Under the direction of IPC, the Office of the Chief Information Officer (OCIO) developed the *IMT Governance Policy* (IMT Policy) to guide the departments. The IMT Policy held the Deputy Ministers accountable for the management of information in their respective departments.

The legislative assembly enacted the *Access to Information and Protection of Privacy Act* (ATIPP) as the paramount legislation to protect the private information of NWT residents collected by the GNWT. In March 2011, the OCIO recommended DIIMS as a tool to address the privacy of information for electronic records while making the GNWT operations more transparent. Subsequently, in 2014, the Corporate Information Management (CIM) group was created in the Department of Infrastructure to implement DIIMS in departments and support electronic records management. The annual operating budget of CIM was approximately \$1.6 million to support 2,300 users.

The primary contacts for the CIM team in the departments were the Record Coordinators. Their primary responsibility was to manage all records under the *Archives Act* and process ATIPP requests. Specific to DIIMS, the Records Coordinators were responsible for:

- managing their department's DIIMS user account creation, account deletion, installation, permissions and training requests
- providing advice and guidance on the acceptable use of DIIMS to management and employees in their departments.

As of November 30, 2019, nine GNWT departments had fully or partially implemented DIIMS. The following departments have not fully implemented DIIMS:

- Education, Culture and Employment
- Executive and Intergovernmental Affairs
- Finance
- Health and Social Services
- Legislative Assembly.

C. OVERVIEW

The GNWT objective of protecting the privacy of information while making the GNWT operations more transparent could be achieved with effective governance and monitoring the use of DIIMS. Supported by a knowledgeable, professional, and proficient CIM team, DIIMS can meet GNWT needs for electronic records created by Microsoft Office Suite and similar software.

The OCIO took a leadership role in selecting the DIIMS application to meet GNWT needs. In establishing the CIM group, an executive-level sponsor with an enterprise-wide mandate to implement, manage, and monitor DIIMS was not identified. The CIM team's on-going concern was the lack of compliance by departments to follow proper DIIMS practices even though over 90% of the DIIMS users had received training.

The current risk assessment of information stored in DIIMS remains very high. The likelihood of non-compliance with DIIMS practices, resulting in inappropriate access to government records, was almost inevitable. While the financial and operational impact could be minor, the reputational impact could be significant. Stakeholder trust might be severely damaged with the release of private information and may also attract national media attention.

To enhance the governance process and internal controls to manage the high-level risk and ensure compliance with ATIPP and the *Archives Act*, IPC could:

- designate a champion to complete the implementation of DIIMS in the GNWT as the designated tool to store government's electronic records
- require a regular update on the status of DIIMS implementation, usage, access monitoring, and compliance based on the Key Performance Indicators approved by IPC for any remediation action.

The audit examination coverage was to November 30, 2019 (**Schedule I refers**). Management responses are as of December 21, 2020. Some of the high-risk areas will be outstanding until March 2022.

D. ACKNOWLEDGEMENT

We want to thank the records management staff in all departments and the Chief Information Officer's Office for their assistance and co-operation throughout the audit.



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Observation 1: Governance- Project Management

Criteria:
<ul style="list-style-type: none">• Governance programs need to be sponsored by executive management - COBIT 2019• The Executive is responsible for the project and gives a single point of accountability for the project. - Prince2• The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal - ATIPP Act, 42
Condition / Evidence
<p>Project management objectives include developing the project's initiation, planning, execution, and closure procedures while achieving the project goals within a specific timeframe and budget. Widely accepted standards such as Prince2 and COBIT state that a project requires an executive sponsor to be the single point of accountability for a project. A recent example in the GNWT includes the SAM Upgrade project conducted by the Finance Department and sponsored by the Comptroller General. The Project Management Institute indicates that active sponsors drive 75% of successful projects.</p> <p>In reviewing the Electronic Records & Document Management System (ERDMS) draft project documentation, we noted that a draft 2008 Project Charter identified the GNWT Chief Information Officer (CIO) as the sponsor for the preliminary analysis phase. Project objectives included performing an analysis of the individual Department's electronic records management needs. The goal was to find a standardized GNWT solution for document management that would provide secure, timely and efficient access to information. This phase was successfully concluded when the preliminary analysis was completed in March 2011.</p> <p>With DIIMS identified as the corporate solution, the project was handed over to the Corporate Information Management (CIM) group. We had expected to find a similar governance structure for the implementation phase of DIIMS. In our discussions with management and review of the project documentation, we noted that:</p> <ul style="list-style-type: none">• There was no signed off Project Charter for the implementation phase, and we were unable to obtain any documentation on the project handover.• An executive sponsor, signifying senior management support, had not been identified for the implementation phase project.• DIIMS was first implemented in 2012. To date, nine departments had fully or partially implemented the system after completing readiness assessments.• Capital expenditure on the DIIMS application amounted to \$2.2 million. Ongoing staff, maintenance and training costs were more than \$1.6 million per year.

Risk/Consequence:	
<ul style="list-style-type: none"> • Return on investment in DIIMS may not be realized. • Project objective to manage records, improve security, and comply with access and privacy legislation may not be fully met. 	<p>Risk Rating: High Likelihood: Almost Certain Impact: Moderate Risk Owner: IPC Chair</p> <p>Support:</p> <ul style="list-style-type: none"> • Chief Information Officer, Finance • Director, Corporate Information Management, Infrastructure • Director TSC
<p>Recommendation:</p> <p>To meet the FMB mandate of fiscal responsibility and accountability, we recommend that the IPC:</p> <ol style="list-style-type: none"> a) Appoint an executive sponsor to complete the implementation of DIIMS in the GNWT. b) Clarify the Corporate Information Management's (CIM) enterprise-level mandate and responsibility for the DIIMS implementation, and their accountability to the IPC for the project's execution. c) Delegate the CIM to develop a plan to complete the DIIMS implementation and provide the CIO with periodic status updates on the project progress. 	
Management Response:	Timeline:
<ol style="list-style-type: none"> a) Assistant Deputy Minister, Programs and Services with the Department of Infrastructure is appointed as the executive sponsor of the implementation of DIIMS across the Government of the NWT. b) CIM will work with Governance Planning and Security to update the Recorded Information Management Policy to include CIM mandates and responsibilities. c) CIM will engage with the Departments of ECE and Health to develop plans to complete the implementation of DIIMS. 	<ol style="list-style-type: none"> a) immediately b) March 2022 c) Discussions with departments to begin in January 2021; plans anticipated to be complete on March 31, 2021.

Observation 2: Governance – Monitoring Role

Criteria:
<ul style="list-style-type: none">• The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal - ATIPP Act, 42• There is a legal framework for disposing, transfer, custody and access to records - Archives Act• Information Management and Technology governance framework - IMT Governance Policy• Government bodies must ensure and be able to demonstrate that electronic information maintains its integrity, is complete, and is not altered by unauthorized parties - Management of Electronic Information Policy• Government bodies will manage recorded information in their custody consistently with this policy and compliance with legislation- recorded Information Management Policy.
Condition/ Evidence:
<p>The FMB delegated the Informatics Policy Council (IPC) the accountability for information management oversight (IM). The CIO supported the IPC by managing overall IM within the Government.</p> <p>The Deputy Heads supported information management by monitoring and reporting on IM objectives within their departments. Records Coordinators were responsible for the implementation of an information management system. This departmental role included providing employees access to DIIMS records based on their roles and with Management approval.</p> <p>In reviewing legislation, policies and conducting interviews with staff. We observed that:</p> <p>a. Policy and Procedures</p> <p>A policy had not been developed, and the standard requiring Departments to use DIIMS for all their electronic records, compatible with the application, had not been approved. As a result, there was no consequence of not using DIIMS for electronic records management.</p> <p>To assess how employees were using the DIIMS application, the IAB surveyed 460 DIIMS users. Employees surveyed included all Operational Managers responsible for monitoring access to records and random samples of staff in departments. The survey response rate was 40%, equaling 200 users. The survey results showed that most employees (93%) had received DIIMS training; however, only 48% had received records management training. Despite the DIIMS training provided to most employees, the survey showed that only 60% were using DIIMS as their primary tool for electronic records management, and 50% continued to save documents on their desktops.</p>

Management Responses As of December 21, 2020

Condition/ Evidence:	
<p>b. Monitoring Access</p> <ul style="list-style-type: none"> ○ The responsibility to assign and monitor access to records within DIIMS had been delegated to the Records Coordinators; however, accountability had not been clearly defined or communicated to the departments. ○ Records Coordinators did not have the hierarchical authority to monitor and enforce adherence to DIIMS records management policies. We did not find evidence of a documented process that would allow the Records Coordinators to identify and escalate inconsistent or inappropriate requests for information. ○ 70% of Records Coordinators indicated that they monitored DIIMS access to their Department's sensitive information. This monitoring was limited to: <ul style="list-style-type: none"> ▪ Actioning items identified in the DIIMS Sensitive Keyword exception report. For example, identifying file names with "offer letter" or "Grievance" that did not have additional markings and were accessible to everyone. ▪ Using the additional marking features to restrict access to files. <p>It was notable that ENR/ITI/Lands group ran weekly DIIMS reports to monitor folders' creation, weekly contributions, and permission changes. Other departments could use a similar process.</p> <ul style="list-style-type: none"> ○ Records Coordinators indicated that most departments did not have a full-time records management resource. Their time was shared between records management and attending to an increasing number of ATIPP requests. 	
Risk/Consequence:	
<ul style="list-style-type: none"> ● ATIPP requirements to protect personal information may not be met. ● Information maintained within DIIMS may be disposed of inappropriately, resulting in non-compliance to the Archives Act. ● IPC unable to assure the FMB that the GNWT's electronic information has a completeness and authentic integrity. 	<p>Risk Rating: Very High Likelihood: Almost Certain Impact: Major Risk Owner: IPC Chair</p> <p>Support:</p> <ul style="list-style-type: none"> ● Chief Information Officer, Finance ● Director, Corporate Information Management, Infrastructure

Management Responses As of December 21, 2020

Recommendation:

To meet the FMB mandate of accountability and transparency, we recommend that the IPC:

- a) Authorize a standard designating DIIMS as the GNWT electronic records management tool and assign roles and responsibilities to monitor its use.
- b) Develop corporate level Key Performance Indicators to demonstrate that effective security and access controls are in place.
- c) Require mandatory records management training for all employees linked to their roles.
- d) Provide Senior Level Managers, delegated with the responsibility for their Department's records management, and Records Coordinators with specialized training on utilizing DIIMS reporting tools to monitor access for the protection of private and confidential information.

Management Response:

Timeline:

- | | |
|--|---|
| a) CIM will work with GPS to finalize and communicate a Directive that has already been developed. | a) May 2022. |
| b) The corporate level Key Performance Indicators will be a roll-up of the departmental KPI's developed by the Records Information Management Committee. These KPI's will be focused on ensuring that departmental information stored in DIIMS is secure and accessible. | b) Discussions to begin in early 2021/22 fiscal year. |
| c) CIM will recommend to the Department of Finance, Human Resources Branch that RM training is included in the list of mandatory training for employees. | c) March 2021 |
| d) CIM will develop on-demand reporting for senior managers and records managers on request. | d) Immediately. |

Observation 3: DIIMS Access Process

Criteria:
<ul style="list-style-type: none">• The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal – ATIPP Act, 42• A consistent approach to recorded information management improves the economy, efficiency, and effectiveness of government programs and services – Recorded Information Management Policy• Corporate Information Management and Records Coordinators roles and responsibilities – DIIMS Handbook
Condition / Evidence:
<p>Requests for any changes to employees' DIIMS access were routed to the DIIMS Help Desk through the Records Coordinators as per operating procedures.</p> <p>We tested DIIMS access controls by verifying the current access for a sample of 30 users that had either been terminated or transferred to other divisions/departments between October 1, 2018, and April 30, 2019. We observed that;</p> <ul style="list-style-type: none">• As of April 30, 2019, four users still had access to their Department's records and were still active in the GNWT Active Directory after their effective termination dates. We confirmed that none of these former employees had accessed DIIMS after their effective termination dates by reviewing their DIIMS audit trail reports.• One user kept DIIMS access across three departments (JUS, EIA and DAAIR). This user was initially approved for multiple accesses to facilitate a transition period after being transferred to a different department; this access was not revoked after the transition period had elapsed.• Records Coordinators routed requests for account creation/change/ deletion to the DIIMS help desk through the requisite forms or emails.<ul style="list-style-type: none">○ The Record Coordinators were only able to provide supporting documentation on 16 of the 30 users.○ Records Coordinators had no knowledge or correspondence regarding the termination or transfer for seven users.• All five Records Coordinators expressed a lack of standard processes within their departments for :<ul style="list-style-type: none">○ Submitting DIIMS access requests/changes○ Communicating and following-up on DIIMS access requests/change○ Filing/retrieving communications regarding DIIMS user access• A weakness identified and confirmed by management was that users self-report any changes to DIIMS access; if the DIIMS team or Records Coordinators were not informed of an employee's move, they could not remove that user's access.

Management Responses As of December 21, 2020

Risk/Consequence:	
<ul style="list-style-type: none"> • Non-compliance to ATIPP as privacy and security of information may be compromised by allowing access to restricted information. • Non-compliance to the Archives Act as documents may be accidentally deleted or modified and vital information lost • GNWT's reputation may be impaired if confidentiality or privacy are violated 	<p>Risk Rating: Very High Likelihood: Almost Certain Impact: Major Risk Owner: Director, Corporate Information Management, Infrastructure Support:</p> <ul style="list-style-type: none"> • Chief Information Officer, Finance • Director of Finance, Departments
Recommendation:	
<p>To meet legislative requirements and the FMB mandate of accountability and transparency, we recommend that the CIM:</p> <p>a) In consultation with Human Resources and the Departments, document the process to advise the DIIMS team on user accounts changes such as the onboarding, transfer, and termination of employees.</p> <p>b) Develop department level Key Performance Indicators to demonstrate that effective security and access controls are in place. These measures would be validated by departmental managers and used to monitor any changes to access.</p>	
Management Response:	Timeline:
<p>a) CIM will continue to engage with HR, TSC, ISSS, Access and Privacy Office, and other stakeholders on streamlining the communications and guidance to Managers around employee onboarding, off-boarding, and transfers to ensure DIIMS access and information management activities complete</p> <p>b) CIM will engage departments through the Records Information Management Committee in developing tools and processes for Key Performance Indicators. CIM will provide direction to departments for DIIMS on-demand access and security reporting. Guidance will be provided on the review protocol, including frequency. Some Key Performance Indicators that departments can use include:</p> <ul style="list-style-type: none"> i. DIIMS Growth vs File share growth report ii. Number of inactive DIIMS user accounts iii. Number of items deleted (outside of regular disposition) 	<p>a) Already in process.</p> <p>b) Discussions to begin in early 2021/22 fiscal year.</p>



CONFIDENTIAL

May 15, 2020

File: 7820-30-GNWT-151-111

MR. SANDY KALGUTKAR
CHAIR, INFORMATICS POLICY COUNCIL
FINANCE

Audit Report: GNWT Information Technology Procurement
Audit Period: April 1, 2017 to March 31, 2018

A. SCOPE AND OBJECTIVES

The Audit Committee approved the Information Technology Procurement (IT procurement) audit in the 2016-2017 Audit Work Plan. The audit scope was the Government of the Northwest Territories (GNWT) Information and Management Technology (IMT) procurement process. The objectives were to determine if:

- an adequate governance framework existed to align IMT procurement with Financial Management Board (FMB) mandate for fiscal responsibility, accountability and transparency
- information required for decision making was reliable, relevant, complete and accurate
- IMT procurement complied with the *Financial Administration Act* (FAA), Financial Administration Manual (FAM), and Informatics Policy Council (IPC) policies and procedures.

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

B. BACKGROUND

FAA, Section 7, assigns the FMB responsibility for the approval of plans, policies and strategies associated with IMT. FAA, Section 9, states the responsibilities of the FMB must be carried out in a manner that promotes and supports fiscal responsibility, accountability and transparency of Government operations.

IPC was established by the FMB to assure that the GNWT's IMT function was managed in accordance with appropriate strategies and policies. The Chief Information Officer (CIO) supported the IPC and was responsible for establishing the management framework for the IMT function.

The CIO works with all stakeholders in all aspects of its mandate to ensure that IMT investments, assets, and operations support the business goals of the GNWT in an effective, efficient and economical manner.

The Office of the Chief Information Officer (OCIO) provides day-to-day guidance to all stakeholders regarding IMT strategy, security and policy implementation. IPC allocated an average \$6.5 million in the annual IMT Capital Fund, and the GNWT incurred an average of \$20 million per year on "computer" expenditures.

Over \$128 million in "computer" expenditure data was recorded in the GNWT financial information system, the System for Accountability and Management (SAM) over six years. This \$128 million did not include other IMT expenditures such as consulting services and internal staff due to insufficient information.

C. OVERVIEW

The rapidly changing nature of IMT complicates the operating environment. The governance of IMT does not need to be complex.

The current GNWT IT procurement systems and processes were fragmented. The IPC provided oversight on IT procurement related to capital expenditure of \$6.5 million annually. The additional GNWT “computer” expenditure of more than \$13 million was shared among departments.

The 2016 FAA assigned FMB with responsibility for IMT plans, policies and strategies to be carried out in a manner that promotes and supports fiscal responsibility, accountability and transparency of Government operations.

Clarification and communication of the existing policy to reinforce the role of OCIO in IT procurement were required. This will allow the OCIO to implement a management framework to enable it to monitor GNWT IMT expenditure and to support the FMB mandate. Implementation of these steps could reduce the overall risk from a “very high” risk to “moderate” risk.

OBSERVATIONS AND RECOMMENDATIONS

1. Governance Framework

The \$20 million annual investment in IT procurement did not have an adequate governance framework to optimize resources.

FAA Section 7.2 states, “... the Board shall act on all matters related to the financial management and financial administration of Government in respect of ...the approval of plans, policies and strategies associated with information management and technology.”

The FMB delegated responsibility for oversight and implementation of IMT governance to the IPC through FAM 115.

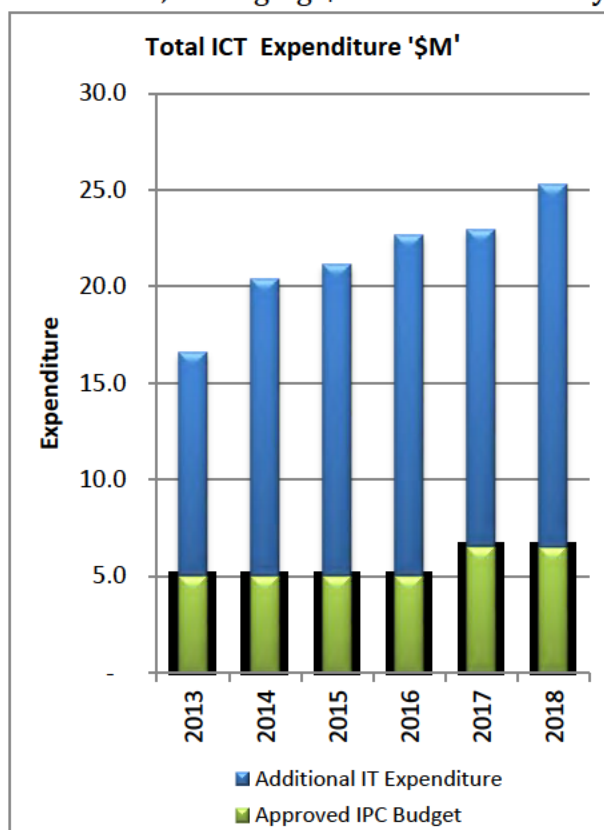
A review of the IT Governance Policy identified that principles such as ensuring benefit, risk and resource optimization, incorporating stakeholder needs and ensuring stakeholder transparency had been incorporated. However, the roles and responsibilities relating to resource optimization, monitoring and enforcing IMT policy had not been defined.

The SAM financial transactions for “computer” expense codes indicated that the GNWT had spent \$128 million from 2013 to 2018, averaging \$20 million annually, as indicated in the chart.

The IPC approved \$6.5 million in annual IMT capital investment, with support from the OCIO. Oversight of the additional \$13.5 million in annual capital and non-capital IMT expenditure was not defined. Departments managed these IMT expenditures within their IT divisions.

The OCIO was not consistently consulted on departments IMT investment decisions: instead acting in an advisory role, as and when requested by departments.

We interviewed thirteen staff from departments, OCIO, Technology Service Center (TSC), and



Procurement Shared Services (PSS) (**Appendix A Refers**). Key issues identified were:

- the departments had a varying understanding of their role and that of the IPC, OCIO, TSC and the PSS concerning IT procurement.
- the IMT capital expenditure process was not consistently followed. Departments found ways to override the requirement of consulting the OCIO.
- support for departments on investing in capital IMT assets was not coordinated between OCIO, TSC and PSS and within departmental divisions.
- there were no consistent standards to assist departments in purchasing IMT products and services, and no formal guidelines on best practices to procure smaller value items.

Clarity on roles and responsibilities would allow for leveraging on existing controls to monitor and enforce compliance to set policies and to optimize resource use for IMT investments.

Risk Profile:

Risk Impact	Very high risk with a major impact requiring detailed plans by senior management.
Risk Responsibility	Informatics Policy Council
Risk Mitigation Support	Office of the Chief Information Officer

Recommendation:

We recommend that the CIO:

- a) In consultation with IPC and Senior Management, enhance the governance framework by clearly defining the monitoring and enforcement roles and responsibilities to optimize resource use.
- b) Develop a communication and implementation plan to circulate the completed governance framework to departments.

Management Response:

Action Plan	Completion Date
a. Subject to the approval of IPC, the Department of Finance will update the IMT Governance Framework to clearly identify the roles and responsibilities for the monitoring and reporting of IMT budgets and expenditures.	<u>July 2020</u>
b. The Department of Finance will communicate roles and responsibilities related to monitoring and reporting of IMT sector budget and expenditure information Within IMT Sector organizations Within Departments	September 2020 January 2021

2. Management Framework

There were no tools to monitor and report on the total annual IMT investment to the FMB.

The FMB delegated the responsibility to establish a management framework for IMT functions to the CIO through the IMT Governance Policy.

A review of the IMT policy suite indicated that the management framework was operating at an ad hoc level and did not capture the full cost of IMT investment. The framework did not define appropriate organizational structures, reporting relationships, roles and responsibilities, standards, performance management or review of IMT budgets for alignment to the strategic direction set by IPC.

During interviews conducted with the OCIO and departmental informatics staff, we noted that:

- there was no reporting mechanism to coordinate IMT investment information to make decisions on managing the GNWT's IT resources.
- information pathways and reporting were inconsistent for department IT initiatives, and approval steps were not clear.
- departments were engaging in the use of IMT enabled systems without explicit approval or knowledge by the OCIO, as reported in the GNWT Cyber Security Resilience report of May 31, 2018.
- the Procurement guidelines did not account for the unique needs of ICT procurements, such as requirements for information security, privacy impact assessment, threat risk assessment, and timing of services.

Analysis of SAM IT expenditure data revealed that IMT expenditure could not be identified easily. TSC captured the full cost of IMT expenditure by tracking hardware, software, consulting, and staffing costs. However, this information was not available on a GNWT wide basis. We noted that some TSC chargebacks had been coded to the wrong expense accounts by various departments (**Schedule 1 Refers**).

The IPC did not have access to complete and accurate information to assure the FMB that IMT investments were managed in a fiscally responsible, accountable and transparent manner. An effective management framework could have prevented:

- confusion over appropriate authority, roles and responsibilities of stakeholders.
- lack of accountability for monitoring and reporting on IMT investment
- inconsistent application of procurement standards on IMT assets
- OCIO lacking visibility into departmental IMT enabled investments

Risk Profile:

Risk Impact	Very high risk with a major impact requiring detailed plans by senior management.
Risk Responsibility	Chief Information Officer
Risk Mitigation Support	Office of the Chief Information Officer

Recommendation:

We recommend that:

- a. The OCIO develop a management framework and define a process for departments to report on IMT activity periodically.
- b. The OCIO conduct an information needs assessment to enable monitoring and enforcement of departments IMT investment activities, PSS and TSC IMT support activities provided to departments.
- c. The OCIO work with the Office of the Comptroller General to define a coding structure in SAM that will enable monitoring of the full cost of IMT expenditure.
- d. The OCIO provide an annual report to the IPC on the overall GNWT IMT investment activity with accurate, complete, reliable and timely information.

Management Response:

Action Plan	Completion Date
a. The Department of Finance will research government best practices and work with other IMT sector organizations to inform the design of the budget and expenditure monitoring and reporting framework.	<u>June 2020</u>
b. Under the updated governance framework, the Department of Finance will work with stakeholders, including DFAs, to design a budget and expenditure monitoring and reporting framework for IMT activity.	<u>July 2020</u>
c. The Department of Finance will work with the Comptroller General to define a coding structure to support budget and expenditure monitoring and reporting and will roll out to:	<u>July 2020</u>
<ul style="list-style-type: none"> • The IMT Sector in phase one (Information Systems 	<u>October 2020</u>

Action Plan	Completion Date
<p>Shared Service, the TSC, NTHSSA, Health and Social Services, Corporate Information Management, FIN-ERPS).</p> <ul style="list-style-type: none"> • Departments in phase two (working with DFAs). <p>d. The Department of Finance will provide an annual report of IMT Budget and Expenditure to IPC.</p>	<p><u>April 2021</u></p> <p><u>Annually</u> <u>(Following year-end close.)</u></p>

D. ACKNOWLEDGEMENT

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



T. Bob Shahi
Director, Internal Audit Bureau
Finance

GNWT Wide
 Information Technology Procurement
 File No. 7820-30-GNWT-151-111
 April 1, 2017 – March 31, 2018
TSC Expenditure Analysis

TSC charge back coded to 'Computer ' expense accounts

Fiscal Year	Department	Account	Account Description	Invoice Description	Invoice ID	Vendor ID	Vendor Name	Amount
2018	EIA	17(1)						
2017	EIA							
2015	FIN							
2014	ENR							
2014	MACA							
2013	ENR							
2013	MACA							
Total								6,344,067

TSC Chargeback miscoded to other expense accounts

Fiscal Year	Department	Account	Account Description	Invoice Description	Invoice ID	Vendor ID	Vendor Name	Amount
2018	LND	17(1)						
2017	LND							
2016	LEG							
2016	ECE							
2013	HR							
Total								635,290

GNWT Wide
Information Technology Procurement
File No. 7820-30-GNWT-151-111
April 1, 2017 – March 31, 2018
Summary of Interviews

APPENDIX A

Interviews were conducted with thirteen staff from GNWT central and departmental Information Management and Technology (IMT) groups. The interviewees indicated that :

- there was no standardized process to follow to assist departments in purchasing IT products and services consistently.
- there were no formal policies and procedures on IT procurement best practices or the procurement process for smaller IT purchases.
- Office of the Chief information Officer's (OCIO) role in GNWT departments was unclear, their role had mostly been advisory for larger IT projects as requested by departments.
- the Technology Service Center (TSC) was often called in by client departments at the eleventh hour when the system or program was not functioning correctly. Ideally, the TSC should be involved right from the start to ensure the system or application is compatible with the GNWT network and server environment.
- Procurement Shared Services (PSS) staff does not always understand the urgency associated with the majority of IT product requests, wait times when dealing with PSS staff could be lengthy .When questioned the staff sometimes responded poorly due to lack of accountability towards the department.
- IT procurement process would improve if the client departments were required to consult with OCIO for IMT goods and services procurement.
- A governance framework needed to be developed to assess departments and overall IT expenditure in a consistent manner that enabled organizational prioritization and assessment.
- The definition of the ' IT asset ' term was not clear in the ICT Policy: accounting asset versus capital asset.
- TSC needs were complex, the addition of an IT specialist within the PSS could help the procurement of IT run more smoothly as the specialist could review specs and the assess the technical side of the system/application before the tender or RFP process.



JAN 18 2017

CONFIDENTIAL

File: 7820-20-GNWT-151-120

MR. DAVID STEWART
DEPUTY MINISTER
FINANCE

GNWT Overtime Review, April 1, 2012 to March 31, 2016

The Audit Committee approved the GNWT-Wide Overtime project as part of the 2015-2016 Audit Work Plan. This letter covers data analysis information specific to the Department of Finance (Finance). Information contained in this letter will be consolidated into the final GNWT-Wide Overtime Audit Report for the Department of Human Resources (DHR).

Summary of Data Analysis

The overtime data analysis was conducted with information available from PeopleSoft for the four year period April 2012 through March 2016. The audit classified overtime as all wages earned above an employee's regular hourly wage.

Data analysis showed that an average of \$486,500 a year was incurred in overtime over the audit period (**Schedule 1 refers**):

- Schedule 1(a) – Gross overtime in Finance
- Schedule 1(b) – Overtime incurred by top 3 sections in Finance
- Schedule 1(c) – Overtime incurred by top 3 overtime codes in Finance
- Schedule 1(d) – Overtime incurred by top 10 employees in Finance

The data provided in Schedule 1 is for informational purposes only for management review.

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

1. Compliance with GNWT overtime policies

The audit expected to find that approved overtime would be compliant with the Collective Agreement and HRM policies. Analysis of data for the audit period revealed four areas that were non-compliant:

- a. Comments field: HRM Section 604, para 7 & 8, requires that the Comments field contain the reason for overtime. Data analysis revealed that 59% (8,386 of 14,306 entries) did not provide any information in the comments column to establish why the overtime was required (**Schedule 2(a) refers**). As a result, management was restricted from conducting any past analysis of the requirement for overtime.
- b. Overtime calculation: HRM 0604, para 14 & 15, required that a minimum payment of one hour be paid at the appropriate overtime rate, and that after the first hour of overtime an employee is to be paid for each completed 15 minutes of time. Data analysis revealed 345 instances over the audit period where OT1, OT1A, and LTE were approved for less than one hour (**Schedule 2(b) refers**). As a result, calculation of all employees' overtime may not be equitable.
- c. Lieu time: HRM Section 609, para 5, specifies that, "Employees may not accumulate more than 75 hours of lieu time per fiscal year (80 hours for employees who work eight hour days)". Data analysis revealed that during the audit period a total of 593 hours of lieu time was banked above the 75/80 hours authorized by the HRM (**Schedule 3(a) refers**). The banking and use of lieu-time above the HRM authorized levels may have created an increased opportunity for overtime for those staff remaining in the workplace.
- d. Banked call-back: HRM Section 0604a, para 19, specifies that overtime earners are to, "Obtain authorization for standby or call-back to be compensated as lieu time". Data analysis revealed that a total of 539 hours of call back time was banked in a separate bank from lieu time (**Schedule 3(b) refers**). Call back was banked under PeopleSoft code CBE (Call back earned) without any governance framework similar to lieu time. The banking and use of call back earned (CBE) created increased opportunity for overtime for those staff remaining in the workplace.

The data analysis observations noted above were not confined to Finance, and were found to varying degrees across all GNWT departments (**Schedule 4 refers**). As indicated above, we will be sharing the data analysis of all GNWT departments with

DHR and making recommendations on corporate issues. A coordinated approach with DHR will allow consistent administrative policies and internal control procedures across GNWT departments.

The details of the information in the schedules have been provided to your staff. Should you require additional information, please feel free to call me at (867) 767-9175, ext. 15215.

Sincerely,



T. Bob Shahi
Director

- c. Mr. Jamie Koe, Chair, Audit Committee
Mr. Terence Courtoreille, Director Corporate Affairs, Finance

GNWT-Wide Overtime Audit
April 1, 2012 to March 31, 2016

1(a) Finance: Total Overtime

Fiscal Year	Earnings
2012-2013	\$ 148,874
2013-2014	\$ 190,880
2014-2015	\$ 805,863
2015-2016	\$ 800,083
Total	\$ 1,945,700
Average / Year	\$ 486,425

1(b) Finance: Top 3 Sections Incurring Overtime

2012-2013			2013-2014			2014-2015			2015-2016		
Section	Section Name	Amount	Section	Section Name	Amount	Section	Section Name	Amount	Section	Section Name	Amount
1501611	Reporting & Collection	\$ 29,576	1500331	Regional Ops	\$ 51,451	1500211	Fin & Admin	\$ 196,680	1502711	Fin Payroll	\$ 119,307
1500331	Regional Ops	\$ 23,597	1500611	FMBS	\$ 28,633	1502711	Fin Payroll	\$ 94,053	1500211	Fin & Admin	\$ 105,767
1500611	FMBS	\$ 18,923	1501611	Reporting & Collection	\$ 23,374	1502811	Benefits Admin	\$ 78,775	1501911	SAM Sustainment	\$ 94,736
Total		\$ 72,096			\$ 103,458			\$ 369,508			\$ 319,810
% of Total Overtime		48%			54%			46%			40%
Average Overtime Earned by Top 3 Sections		\$ 216,218			44%						

1(c) Finance: Top 3 Types of Overtime

2012-2013			2013-2014			2014-2015			2015-2016		
Overtime Code	Overtime Name	Amount	Overtime Code	Overtime Name	Amount	Overtime Code	Overtime Name	Amount	Overtime Code	Overtime Name	Amount
LT2	Lieu Hours Taken	\$ 39,995	OT4	Overtime @ 1.5	\$ 70,997	OT1	Overtime @ 1.5	\$ 197,564	OT1	Overtime @ 1.5	\$ 163,467
OT4	Overtime @ 1.5	\$ 34,620	LT2	Lieu Hurs Taken	\$ 34,977	LT2	Lieu Hours Taken	\$ 143,175	LT2	Lieu Hours Taken	\$ 124,724
LTX	Lieu Hours Taken	\$ 24,949	LTX	Lieu Hours Taken	\$ 28,958	OT4	Overtime @ 1.5	\$ 85,372	OT4	Overtime @ 1.5	\$ 108,640
Total		\$ 99,564			\$ 134,932			\$ 426,111			\$ 396,831
% of Total Overtime		90%			90%			92%			92%

1(d) Finance: Top 10 Employees

2012-2013	2013-2014	2014-2015	2015-2016
23(2)(f)	23(2)(f)	23(2)(f)	23(2)(f)
Top 10 Employees	\$ 92,834	\$ 119,877	\$ 230,679
% of Total Overtime	62%	63%	29%
Average Overtime Earned by top 10 employees:	\$ 168,152		

GNWT-Wide Overtime Audit
April 1, 2012 to March 31, 2016

2(a) Finance: Comments Field

Year	# of Overtime Approvals	# without any Comments Provided	% Without any Comment
2012-2013	360	208	58%
2013-2014	1,309	821	63%
2014-2015	6,837	4,109	60%
2015-2016	5,800	3,248	56%
Total	14,306	8,386	59%

2(b) Finance: Overtime: Approvals less than 1 hour

Overtime Type:	# Approvals < 1 hour		Total
	LTE	OT1/OT1A	
2012-2013	18	2	20
2013-2014	8	20	28
2014-2015	99	124	223
2015-2016	29	45	74
Total	154	191	345

3(a) Finance: Lieu Time Earned (LTE) > 75 hours

Year	Hours
2012-2013	61
2013-2014	40
2014-2015	247
2015-2016	245
Total Hours:	593

Finance: Lieu Time Earned by Employee > 75 hours

2012-2013	2013-2014	2014-2015	2015-2016
23(2)(d)	23(2)(d)	23(2)(d)	23(2)(d)
Total Hours	61	40	247
			245

3(b) Finance: Call Back Earned/Banked (CBE) Hours

Year	Hours
2012-2013	0
2013-2014	0
2014-2015	261
2015-2016	278
Total Hours:	539

Finance: Call Back Earned/Banked by Employee (hours)

2012-2013	2013-2014	2014-2015	2015-2016
		23(2)(d)	23(2)(d)
Total Hours:	0	261	278

GNWT-Wide Overtime Audit
 April 1, 2012 to March 31, 2016

All GNWT Departments	Year				Total	Average/Year over Audit Period
	2012-2013	2013-2014	2014-2015	2015-2016		
Total Overtime (\$)	\$12,283,958	\$13,236,155	\$13,756,846	\$14,315,097	\$53,592,056	\$13,398,014
Lieu Time Earned Above 75/80 hour limit (hours)	3,757	3,639	3,516	4,735	15,647	3,912
Call-Back Banked outside of Lieu-Time Governance (hours)	1,875	1,404	1,412	1,279	5,970	1,493
Comment Field Populated (% of all approvals)	25%	26%	23%	25%	N/A	25%
Overtime Approved < 1 hour, LTE/OT1 (# of approvals)	340	1,229	1,300	1,299	4,168	1,042



FEB 05 2018

CONFIDENTIAL

MR. DAVID STEWART
DEPUTY MINISTER
FINANCE

GNWT Wide Overtime Audit - April 1, 2012 to March 31, 2016

Enclosed is the above referenced Audit Report.

The Internal Audit Bureau will schedule a future follow-up audit. However, in the interim, we would like to be notified of any progress in implementing the changes to regulations, policy, or practices by July 31, 2018.

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

T. Bob Shahi
Director, Internal Audit Bureau,
Finance

c. Mr. Jamie Koe, Chair
Internal Audit Committee, Finance

Ms. Tara Hunter
Deputy Secretary of Human Resources, Finance

Mr. Terence Courtoreille
Director, Shared Corporate Services, Finance



GNWT-WIDE

Overtime Audit
April 1, 2012 to March 31, 2016

Internal Audit Bureau – Audit Report
February 2018



Audit Report Operational Audit

**GNWT-WIDE
Overtime Audit
April 1, 2012 to March 31, 2016**

February 2018

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



CONFIDENTIAL

February 5, 2018

File: 7820-20-GNWT-151-120

MR. DAVID STEWART
DEPUTY MINISTER
FINANCE

GNWT-Wide Overtime: April 1, 2012 to March 31, 2016

A. SCOPE AND OBJECTIVES

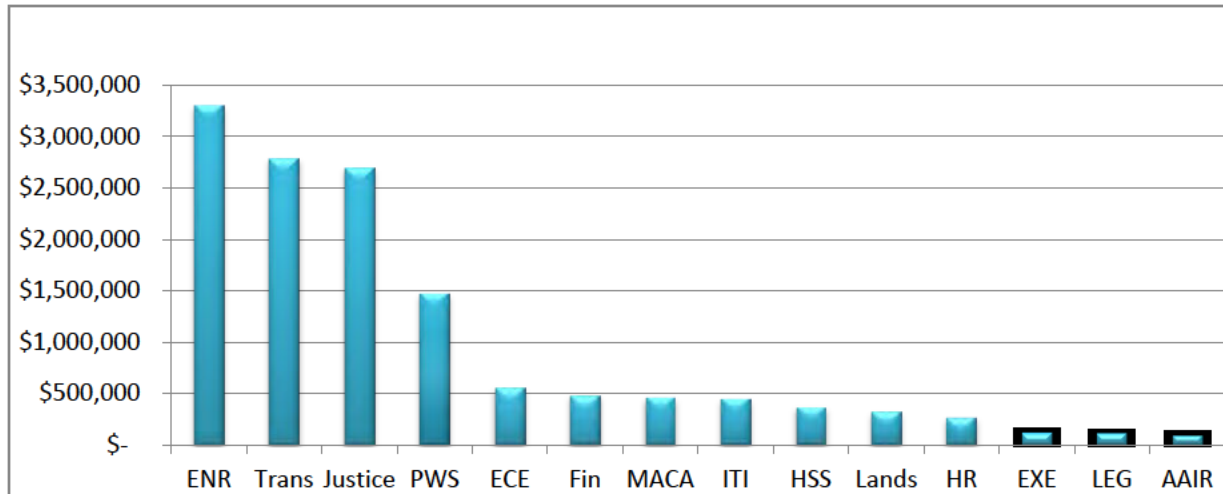
A review of overtime recorded and paid by all departments was approved by the Audit Committee. We conducted analysis of overtime data in Human Resource Information System (PeopleSoft) to assess the level of compliance in recording and processing of overtime transactions.

Department specific results of overtime data analysis have been shared with each department. This report consolidates all departmental overtime data and identifies areas that merit attention by Department of Finance (the Department) in discharging their Human Resources mandate.

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

B. BACKGROUND

Departments recorded an average of over \$13 million in overtime annually for the last four years (**Schedule I refers**). The annual average overtime ranged from \$100,000 to over \$3.3 million:



The Department was responsible for the dissemination of the GNWT overtime governance framework:

- the *Public Service Act*
- Public Service Regulations (Regulations)
- UNW Collective Agreement
- Excluded Employees Handbook
- Human Resource Manual (HRM)
- the Memorandum of Agreement (MOA) between the GNWT and the Union of Northern Workers (UNW) concerning rest periods.

Overtime was considered as all wages earned above an employee's regular hourly wage. The HRM required that overtime be authorized in advance by the responsible manager/approving officer. After the overtime had been worked, the employee was to data enter the overtime and note the reasons for the overtime in the Comments field. Overtime was to be approved within PeopleSoft once the approver had confirmed the reason for the overtime and checked for compliant with the GNWT policy framework.

During the four year period under review, PeopleSoft processed over 400,000 overtime transactions using 55 codes which included items such as call back, lieu hours taken, standby, and 3rd weekend worked premiums (**Schedule II refers**).

C. OVERVIEW

PeopleSoft has been used to record employee compensation for almost two decades. PeopleSoft has the capacity to handle a large volume of transactions from multiple users and approves. The system was able to generate reliable information that we previously audited with little to no discrepancy. The same data analysis tool used for this project was used in our 2009 audits and for the 2015 Health & Social Service Authorities Overtime audit.

The GNWT corporate risk for overtime was high based on processing over 400,000 transactions annually that totaled an average of over \$13 million involving over 4,000 employees in all departments and regions. Non-compliance to overtime policies and procedures impacted financial, operational, and reputation risks. To manage the high risk, GNWT required internal control that were well defined, documented, and monitored.

With the pending revision of *Public Service Act* and associated Regulations, there could be an opportunity to streamline current practice, such as the overtime rate or payment of overtime to professionals and managers, with the legislative framework.

There was limited evidence that overtime approvers were exercising due diligence in approving overtime. Over 75% of the Comment fields were not completed. A documented process to hold the overtime approvers accountable for their role and responsible did not exist. There was no monitoring of the Comment field for compliance.

Specific responsibility needs to be assigned in monitoring the level of compliance to HRM and MOA in the areas of Lieu time, Call-back, and rate of overtime payment.

To effectively manage and monitor the GNWT corporate overtime requires co-ordination effort from number of stakeholders:

- Human Resources to develop the framework in consultation with the departments
- Information Shared Services to generate reliable information for the dashboards
- departments to use the dashboard information to monitor and take any corrective action.

D. OBSERVATIONS AND RECOMMENDATIONS

1. Public Service Regulations

Over five million dollars in overtime was paid annually in non-conformance with Regulations.

Regulations 10(2) and 10(3), Overtime and Holidays, states that employees, other than a manager or a professional, shall be paid overtime when working 0.5 hours or more in excess of the daily or weekly standard hours or when require to work on a holiday, at 1.5 times the regular pay rate.

For the last four years, PeopleSoft code OT2 was used to record payment of overtime at two times the regular pay rate averaging over \$4 million annually.

Fiscal Year	Amount
2012-2013	\$3,816,554
2013-2014	4,105,633
2014-2015	4,269,583
2015-2016	4,386,801
Total	\$16,578,571

Regulations 10 (2) and 10(3) indicated that a manager or a professional should not be paid overtime. The Regulations state:

- Manager: *“means an employee responsible for planning, organizing, coordinating, directing and controlling the use of persons, material and money”*
- Professional: *“means an employee engaged in work where there was a requirement for a highly developed or specialized body of knowledge acquired through university education”*.

An analysis of a sample of 48 Excluded Employees' classified as managers and/or professionals showed that overtime totaling \$1.3 million was earned in 2015-2016 (**Schedule III refers**). Data analysis coding did not allow us to create a complete list of managers and/or professionals who earned overtime over the four year period.

Current UNW Collective Agreement and HRM policies were implemented without ensuring they were consistent with the Regulations.

Risk Profile:

Risk Impact	Major impact requiring senior management research and regulatory changes.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Deputy Secretary HR

Recommendation:

We recommend that the Department work to streamline the Regulations and current overtime practices.

Management Response:

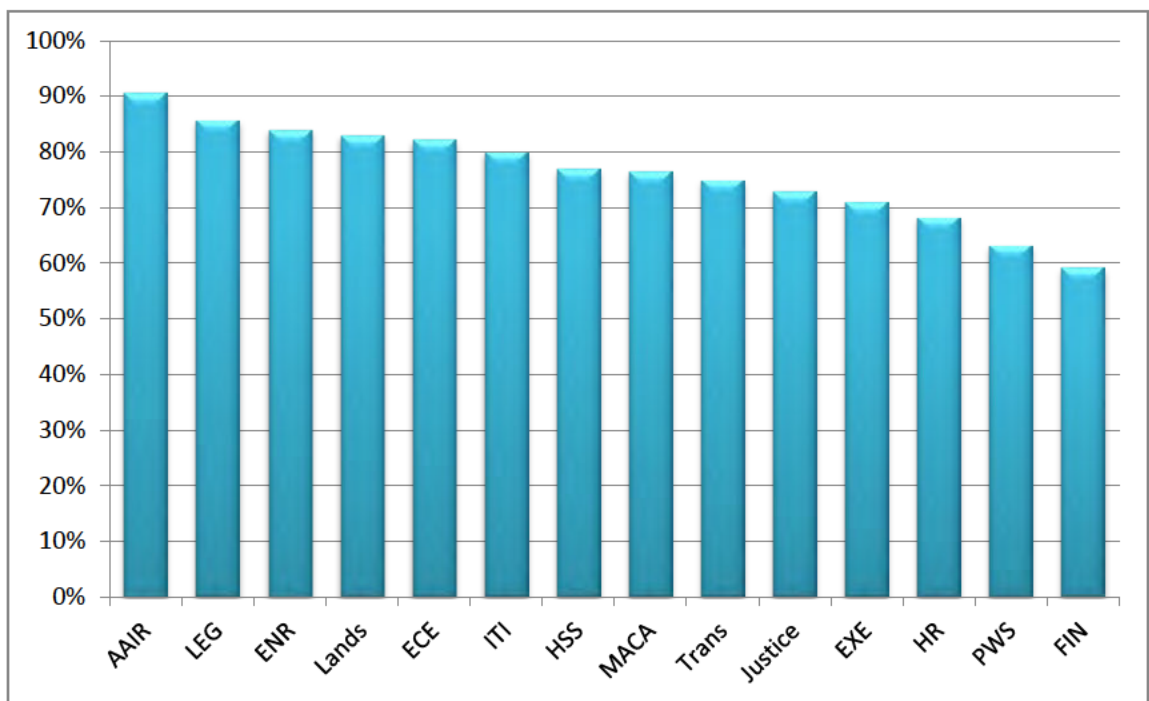
Action Plan	Completion Date
Complete legislative initiative to review and update the Public Service Act and accompanying regulations.	March 2019

2. PeopleSoft Comments Field

Overtime approvers did not exercise due diligence in approving over 75% of overtime transactions.

HRM 604, paragraph 7(4) requires that approvers review and confirm the reasons for the overtime provided by the employee in the Comments field of PeopleSoft Self Service before approving the overtime. The completed Comment fields would be a source of information to allow management to conduct evidence based analysis of overtime usage.

Data analysis showed that the PeopleSoft Comments fields were not completed in over 75% of the transactions (314,300 of 417,800 transactions) (**Schedule IV refers**). There was fair amount of consistency in completing the Comment fields by each department over the four year period. The level of non-compliance among departments ranged from an average of 59% to 91%:



The levels of Comment field completion were consistent with a similar finding from our 2009 overtime audits. Effective April 2014, HRM 604 was updated to make overtime approvers responsible for ensuring the completion of Comment field by employees. However, the risk mitigation steps were not effective as:

- The changes to HRM 604 outlining the overtime approver

- requirements were not widely disseminated
- There was no process in place to hold the overtime approver accountable for their role and responsibility in approving overtime.

Data analysis also showed that information was inconsistent and not susceptible to meaningful analysis for the nearly 25% of the completed Comment fields.

Risk Profile:

Risk Impact	Moderate impact requiring management monitoring of HR resources.
Risk Responsibility	Deputy Minister
Risk Mitigation Support	Deputy Secretary HR Departmental DFA's Department of Finance Information Shared Services

Recommendation:

We recommend that the Department:

- Communicate to PeopleSoft time approvers about the HRM 604 requirements.
- Establish a process that would allow departments to assess the level of compliance to HRM 604.
- Liaise with Information Shared Services to determine the feasibility of establishing a drop down menu for the Comments field with a list of predefined reasons/events that management supports for overtime.

Management Response:

Action Plan	Completion Date
a. Initiate further communication to all PeopleSoft approvers to reinforce requirements under HRM 604.	March 31, 2018
b. The Department will further investigate the ability for departments to assess the level of compliance to HRM 604	March 31, 2018
c. The Department will promote the new functionality for pre-approval of overtime in HRIS and review the data going forward.	On-going

3. Rest Period Memorandum of Agreement

Data analysis indicated that UNW employees may not have followed the Memorandum of Agreement (MOA) requirements on more than 300 occasions annually.

The *Employment Standards Act* exempted all GNWT employees from maximum hours of work requirement specified in the legislation. The April 1, 2014 MOA was to bridge the gap by protecting UNW employees from being subjected to excessive hours of work, both weekly and/or daily. Specifically, paragraph 1.07 states that "*No employee shall work more than 16 consecutive hours*". No formal guidance exists to cover the gap in *Employment Standards Act* for Excluded Employees.

Two years of data analysis identified 688 instances where UNW employees may have worked longer than 16 consecutive hours in a day:

- 347 times in 2014-2015
- 341 times in 2015-2016

UNW employees who worked greater than 16 consecutive hours per day were exposed to greater occupational health and safety risks. Compliance with the MOA was not being respected or enforced by overtime approvers and departmental managers responsible for authorizing overtime.

Risk Profile:

Risk Impact	Moderate impact requiring management planning of available human resources.
Risk Responsibility	Deputy Secretary HR
Risk Mitigation Support	Labour Relations

Recommendation:

We recommend that the Department provide to departments a quarterly report that identifies potential non-compliance with rest period MOA for further investigation.

Management Response:

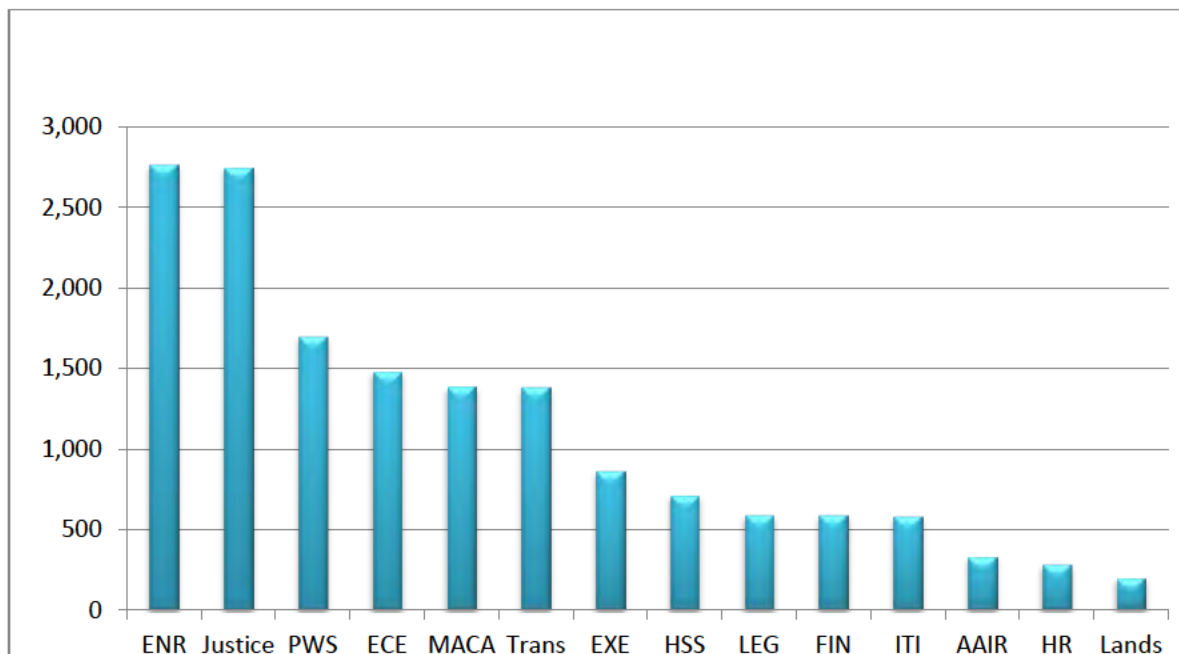
Action Plan	Completion Date
The Department agrees to provide quarterly reporting that identifies potential non-compliance with rest period MOA for further investigation	June 30, 2018

4. Lieu-time Banked

Over 3,900 hours of Lieu-time Earned leave (LTE) was accrued annually above the authorized limit.

HRM 609, paragraph 5 requires that employees may not accumulate more than 75 hours of lieu time per fiscal year (80 hours for employees who work eight hour days).

Data analysis over the four years showed that 7% of LTE (15,647 of 221,381 LTE hours) was accrued above the 75 hours limit (**Schedule V refers**). On the average, over 3,900 LTE hours were accrued above the limit annually. The total accumulated LTE for each department over four years ranged from 200 to 2,700 hours:



The use of banked time as paid leave from work increased the risk for overtime for those staff remaining in the workplace. Fewer employees available within a busy and demanding workplace may necessitate increased overtime for the remaining employees to sustain operational demands.

The information on accumulated LTE for employee was available on ad-hoc basis:

- Overtime approvers may ensure the banking of lieu time was in compliance with the HRM 609 when approving overtime

- departments may request information from Human Resource Manager on the status of LTE in the department.

We did not find a defined process to monitor accumulated LTE at the department level.

Risk Profile:

Risk Impact	Moderate impact requiring management monitoring of HR regulatory compliance.
Risk Responsibility	Deputy Secretary HR
Risk Mitigation Support	Departmental DFA's Information Shared Services

Recommendation:

We recommend that the Department:

- Communicate to PeopleSoft time approvers about the requirement of HRM 609.
- Work in concert with Information Shared Services to provide departments with appropriate dashboard information that would assist in monitoring compliance with HRM 609.
- Liaise with departments to determine if the current limits on lieu-time authorized to be banked continues to be appropriate.

Management Response:

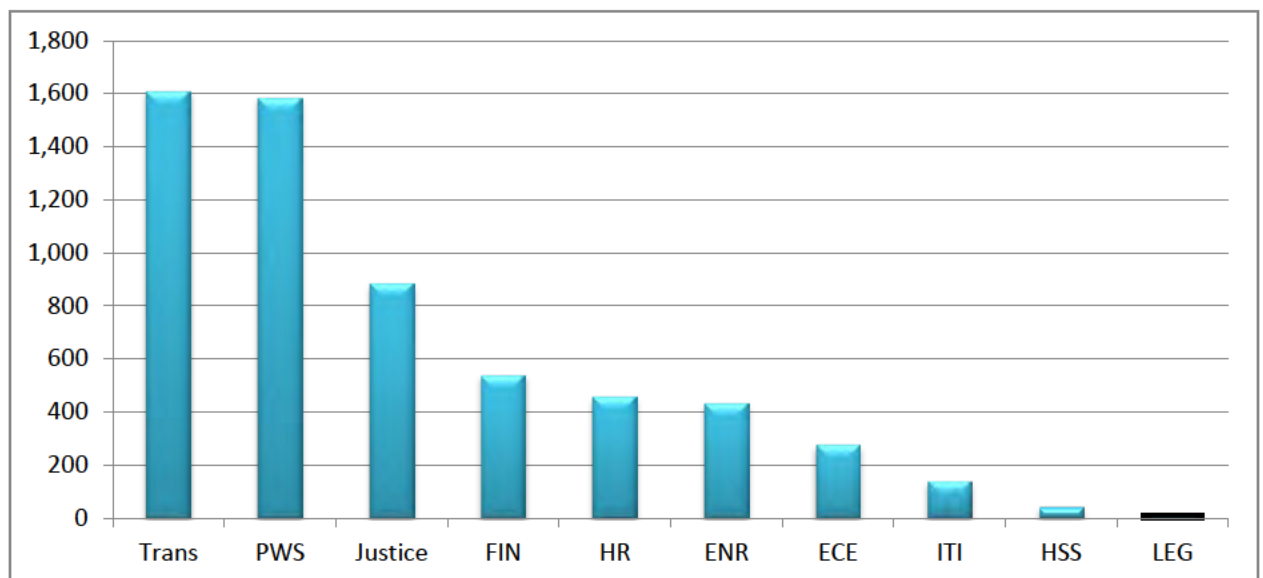
Action Plan	Completion Date
Issue to be further clarified through collective bargaining and finalization of a grievance related to this matter.	Not applicable

5. Call Back Leave

About 1,500 hours of Call Back Earned leave (CBE) was accrued annually.

HRM 604a, Standby and Call-back, paragraph 19 required that employees obtain authorization for call-back to be compensated as lieu time. Lieu time requirement was that employees may not accumulate more than 75 hours of lieu time per fiscal year (Observation 4 refers). There was no other specific governance framework for the use or management of CBE.

Data analysis showed that over the four years a total of 5,970 hours of CBE was approved (**Schedule VI refers**). Only eight departments had CBE recorded and two departments accounted for more than half the CBE:



Call back was tracked as 'CBE, distinct from "LTE" banked leave. There was a risk of accruing and using CBE banked leave outside the HRM 604 guidance.

The use of banked time as paid leave from work increased the risk for overtime for those staff remaining in the workplace. Fewer employees available within a busy and demanding workplace may necessitate increased overtime for the remaining employees to sustain operational demands.

Risk Profile:

Risk Impact	Moderate impact requiring management monitoring of HR regulatory compliance.
Risk Responsibility	Deputy Secretary HR
Risk Mitigation Support	Departmental DFA's

Recommendation:

We recommend that the Department:

- a. Make an assessment of tracking CBE in conjunction with LTE and the impact it would have on the maximum accumulated hour limit.
- b. Communicate to PeopleSoft time approvers about the requirement of HRM 604a.
- c. Work in concert with ISS to provide departments with appropriate dashboard information that would assist in monitoring compliance with HRM 609a.

Management Response:

Action Plan	Completion Date
<p>a, b, & c.</p> <p>The Department will initiate a review and provide direction across all departments as to whether a separate call back bank should exist or whether all lieu time earned should be entered under the one lieu time bank.</p> <p>The Department will work with ISS to investigate if dashboard information can be practicably implemented.</p>	<p>June 30, 2018</p>

6. Overtime Compensation

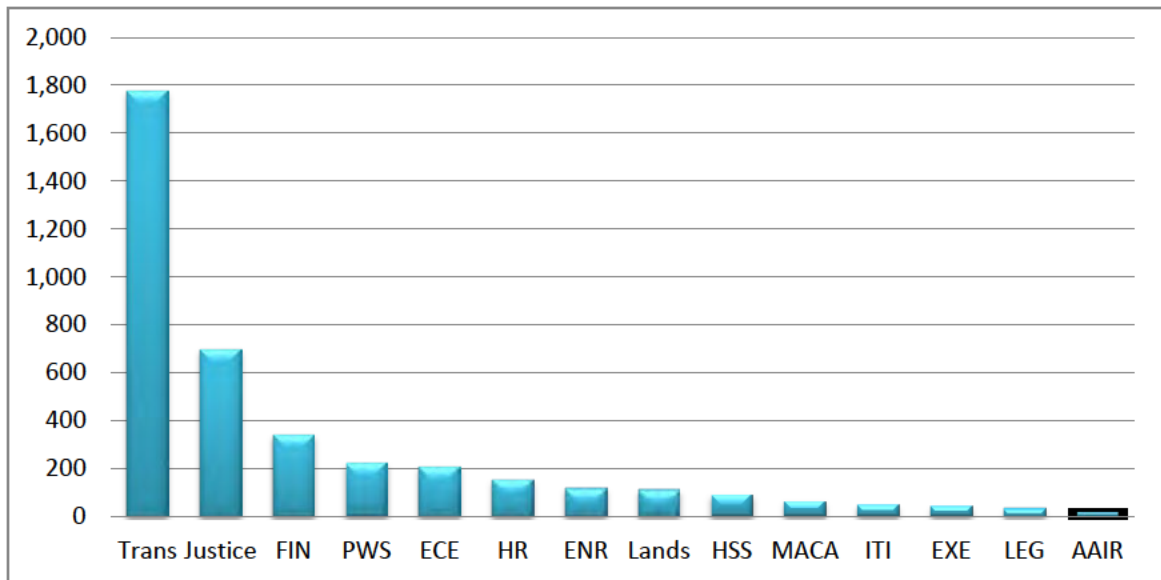
Employees were under compensated for worked overtime at an average rate of about 1,500 times a year.

UNW Collective Agreement, Article 23.05, and the Excluded Employee' Handbook, Hours of Work – Overtime, provides specifics on the threshold and the level of overtime rate to be paid:

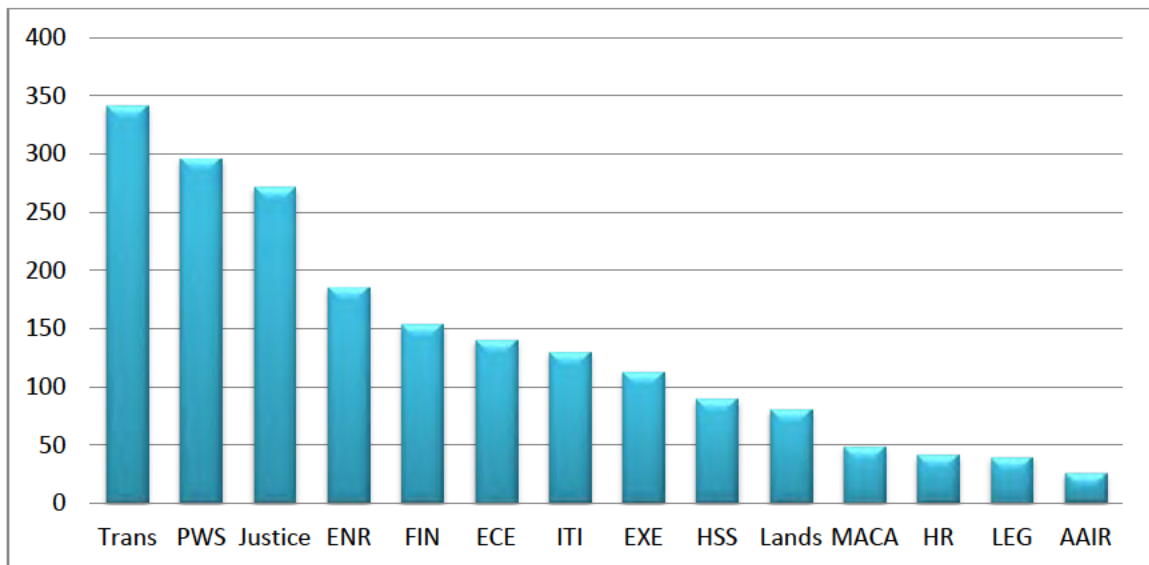
- a. a minimum of one hour of overtime was to be paid for overtime worked
- b. overtime was to be paid at double the regular pay rate after working four hours consecutively.

Data analysis for the four years identified 3,990 transactions where less than less than one (1) hour was processed. Data analysis also identified 1,963 transactions when employees worked overtime for periods longer than four (4) hours but were compensated at 1.5 times base pay (**Schedule VII refers**).

The approval of overtime for less than 1 hour varied widely across departments from 20 times to over 1,700 times over four years:



Approval of overtime rate at 1.5 times base for over 4 hours of consecutive work was consistent over four years for most departments. However, there was variance in this area among departments. This was primarily accounted for by the number of overtime transactions processed in that department:



Approval of overtime remuneration was not performed equitably across all employees for the overtime hours worked and could be subject to grievance by employees individually or as a collective union issue.

Individuals responsible for approving overtime in PeopleSoft did not ensure the approval of overtime hours worked was in compliance with the governance framework.

Risk Profile:

Risk Impact	Moderate impact requiring management monitoring of HR regulatory compliance.
Risk Responsibility	Deputy Secretary HR
Risk Mitigation Support	Departmental DFA's

Recommendation:

We recommend that the Department:

- a. Communication to PeopleSoft time approvers about the requirement of UNW Collective Agreement section 23.05 and the Excluded Employees' Handbook section 'Hours of Work – Overtime'.
- b. Review overtime approvals on a quarterly basis for compliance and brief departments on the status of any non-compliance.

Management Response:

Action Plan	Completion Date
<p>a & b.</p> <p>The Department will include additional messaging to reaffirm the parameters regarding OT entitlements and corresponding PeopleSoft entries.</p> <p>The Department will work with ISS to investigate if PeopleSoft can be customized to only allow for one hour entry for any time initially worked less than one hour.</p>	<p>June 30, 2018</p>

E. ACKNOWLEDGEMENT

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



T. Bob Shahi
Director, Internal Audit Bureau
Finance

GNWT-Wide Overtime Audit
 Departmental Overtime
 April 1, 2012 to March 31, 2016

Schedule I

Department	Year				Total Overtime over Audit Period	Average Yearly Overtime over Audit Period	
	2012-2013	2013-2014	2014-2015	2015-2016			
Environment & Natural Resources	ENR	\$ 2,930,090	\$ 2,942,879	\$ 3,800,806	\$ 3,557,762	\$ 13,231,537	\$ 3,307,884
Transportation	Trans	\$ 2,928,880	\$ 2,799,713	\$ 2,665,643	\$ 2,776,906	\$ 11,171,142	\$ 2,792,786
Justice	Justice	\$ 2,472,679	\$ 3,275,092	\$ 2,306,794	\$ 2,751,789	\$ 10,806,354	\$ 2,701,589
Public Works & Services	PWS	\$ 1,346,324	\$ 1,370,250	\$ 1,487,417	\$ 1,706,972	\$ 5,910,963	\$ 1,477,741
Education, Culture & Employment	ECE	\$ 569,112	\$ 593,803	\$ 595,260	\$ 491,322	\$ 2,249,497	\$ 562,374
Finance	Fin	\$ 148,874	\$ 190,880	\$ 805,863	\$ 800,083	\$ 1,945,700	\$ 486,425
Municipal & Community Affairs	MACA	\$ 405,149	\$ 487,481	\$ 489,911	\$ 486,684	\$ 1,869,225	\$ 467,306
Industry, Tourism and Investment	ITI	\$ 397,193	\$ 316,045	\$ 493,231	\$ 610,389	\$ 1,816,858	\$ 454,215
Health and Social Services	HSS	\$ 293,567	\$ 403,651	\$ 400,559	\$ 409,576	\$ 1,507,353	\$ 376,838
Lands	Lands	NA	NA	\$ 312,609	\$ 337,723	\$ 650,332	\$ 325,166
Human Resources	HR	\$ 469,901	\$ 385,550	\$ 110,043	\$ 116,738	\$ 1,082,232	\$ 270,558
Executive	EXE	\$ 93,038	\$ 212,964	\$ 84,861	\$ 95,247	\$ 486,110	\$ 121,528
Legislature	LEG	\$ 106,155	\$ 138,455	\$ 106,243	\$ 113,498	\$ 464,351	\$ 116,088
Aboriginal Affairs/Intergovernment Relations	AAIR	\$ 122,996	\$ 119,392	\$ 97,606	\$ 60,408	\$ 400,402	\$ 100,101
Total Overtime		\$ 12,283,958	\$ 13,236,155	\$ 13,756,846	\$ 14,315,097	\$ 53,592,056	\$ 13,398,014
GNWT Four Year Increase in Overtime :		16.5%					

GNWT-Wide Overtime Audit
Overtime by PeopleSoft Earning Code
April 1, 2012 to March 31, 2016

Schedule II

Overtime by PeopleSoft Earning Code

	Earning Code		2012-2013	2013-2014	2014-2015	2015-2016	Average Yearly Overtime
1	OT2	Overtime @ 2.0	\$ 3,816,554	\$ 4,105,633	\$ 4,269,583	\$ 4,386,801	\$ 4,144,643
2	OT1	Overtime @ 1.5	\$ 3,134,629	\$ 3,371,501	\$ 3,728,376	\$ 3,788,364	\$ 3,505,718
3	LT2	Lieu Hours Taken	\$ 1,616,707	\$ 1,715,110	\$ 1,964,182	\$ 2,298,595	\$ 1,898,649
4	SBU	Stndby Unwrkd 1.5X H	\$ 697,221	\$ 708,541	\$ 805,466	\$ 830,287	\$ 760,379
5	SBW	Standby Worked	\$ 583,756	\$ 595,187	\$ 637,750	\$ 657,036	\$ 618,432
6	OT4	Overtime @ 1.5	\$ 351,326	\$ 381,332	\$ 326,692	\$ 396,254	\$ 363,901
7	LTX	Lieu Time Taken	\$ 353,178	\$ 390,682	\$ 340,639	\$ 337,408	\$ 355,477
8	CB1	Callback @ 1.0	\$ 329,694	\$ 322,636	\$ 309,095	\$ 311,674	\$ 318,275
9	OT3	Overtime @ 1.0	\$ 255,731	\$ 351,215	\$ 289,785	\$ 342,144	\$ 309,719
10	OT5	Overtime @ 2.0	\$ 208,997	\$ 229,437	\$ 184,925	\$ 213,230	\$ 209,147
11	LT3	Lieu Time Payout	\$ 199,731	\$ 212,140	\$ 219,185	\$ 170,143	\$ 200,300
12	OP2	3rd wknd 4hr+ @ 2 8U	\$ 110,555	\$ 179,233	\$ 7,616	NA	\$ 99,135
13	SBV	Stndby Unwrkd 1.5X H	\$ 67,698	\$ 72,126	\$ 74,237	\$ 86,804	\$ 75,216
14	SBX	Standby Worked	\$ 58,090	\$ 64,020	\$ 62,449	\$ 71,788	\$ 64,087
15	OR2	3rd Weekend over 4 hrs	NA	NA	\$ 77,075	\$ 50,607	\$ 63,841
16	OP1	Reg @ 1.5 (3rd wknd 4 hr)	\$ 62,293	\$ 114,531	\$ 3,743	NA	\$ 60,189
17	CB4	Banked Call Back Taken	\$ 70,762	\$ 61,058	\$ 57,081	\$ 45,284	\$ 58,546
18	CL2	Compensatory Leave Taken	\$ 44,228	\$ 45,016	\$ 44,889	\$ 36,255	\$ 42,597
19	RD2	Resp. Allow OT2 @ 10%	\$ 32,222	\$ 44,553	\$ 34,621	\$ 41,959	\$ 38,339
20	OP0	Reg @ 2.0 (3rd wknd 4 hr)	\$ 52,549	\$ 23,691	NA	NA	\$ 38,120
21	ECB	Electronic Call Back	\$ 29,125	\$ 28,817	\$ 35,599	\$ 32,795	\$ 31,584
22	CB2	Callback @ 1.5	\$ 28,256	\$ 23,750	\$ 31,159	\$ 41,374	\$ 31,135
23	LT4	Lieu Time Payout	\$ 17,287	\$ 31,458	\$ 42,666	\$ 16,738	\$ 27,037
24	CB6	Callback @ 1.0	\$ 25,197	\$ 27,272	\$ 31,372	\$ 18,064	\$ 25,476
25	OR1	3rd Weekend 1st 4 hrs	NA	NA	\$ 30,305	\$ 17,664	\$ 23,985
26	CB3	Callback @ 2.0	\$ 16,360	\$ 11,991	\$ 15,945	\$ 20,576	\$ 16,218
27	RD4	Resp. Allow OT2 @ 12%	\$ 11,718	\$ 15,670	\$ 18,247	\$ 10,202	\$ 13,959
28	LTV	Lieu Time Taken	\$ 8,853	\$ 16,594	\$ 14,705	\$ 11,472	\$ 12,906
29	OT6	Overtime @ 1.0	\$ 13,888	\$ 19,014	\$ 7,283	\$ 8,947	\$ 12,283
30	ECD	Electronic Call Back (1.5)	\$ 10,173	\$ 12,926	\$ 15,636	\$ 9,597	\$ 12,083
	25 other overtime codes		\$ 77,180	\$ 61,021	\$ 76,540	\$ 63,035	\$ 277,776
	Total Overtime		\$ 12,283,958	\$ 13,236,155	\$ 13,756,846	\$ 14,315,097	\$ 13,398,014

Top 3 Overtime Codes:	\$	9,549,009
% of Total Overtime:		71%

GNWT-Wide Overtime Audit
 April 1, 2012 to March 31, 2016

Schedule III

Managers/Professionals **

2015-2016: Overtime (OT1, OT2) and Lieu-Time

	Department	Position	Earnings	Hours
1	Finance	23(2)(f)		
2	Justice			
3	Transportation			
4	Justice			
5	Transportation			
6	Finance			
7	Housing Corporation			
8	Human Resources			
9	Energy & Natural Resources			
10	Legislature			
11	Finance			
12	Transportation			
13	Transportation			
14	Aboriginal Affairs			
15	Justice			
16	Legislature			
17	Legislature			
18	Transportation			
19	Justice			
20	Industry, Tourism and Investment			
21	Public Works & Services			
22	Justice			
23	Finance			
24	Legislature			
25	Justice			
26	Finance			
27	Aboriginal Affairs			
28	Industry, Tourism and Investment			
29	Executive			
30	Transportation			
31	Health and Social Services			
32	Human Resources			
33	Industry, Tourism and Investment			
34	Finance			
35	Justice			
36	Finance			
37	Legislature			
38	Legislature			
39	Aboriginal Affairs			
40	Education, Culture & Employment			
41	Executive			
42	Aboriginal Affairs			
43	Aboriginal Affairs			
44	Human Resources			
45	Human Resources			
46	Transportation			
47	Justice			
48	Lands			
Total Over Audit Period			\$ 1,348,405	

**: Managerial and Professional Employees
 Only Excluded Employees Reported
 Sample limited to 48 employees

GNWT-Wide Overtime Audit
 OT Approvals (%) Without Consent
 April 1, 2012 to March 31, 2016

Schedule IV

Department		Year				Average
		2012-2013	2013-2014	2014-2015	2015-2016	
Aboriginal Affairs/Intergovernment Relations	AAIR	92%	95%	92%	84%	91%
Legislature	LEG	85%	79%	88%	91%	86%
Environment & Natural Resources	ENR	70%	87%	91%	88%	84%
Lands	Lands	NA	NA	85%	81%	83%
Education, Culture & Employment	ECE	83%	85%	80%	81%	82%
Industry, Tourism and Investment	ITI	79%	75%	83%	83%	80%
Health and Social Services	HSS	80%	78%	78%	72%	77%
Municipal & Community Affairs	MACA	67%	72%	81%	86%	77%
Transportation	Trans	80%	76%	73%	71%	75%
Justice	Justice	74%	70%	75%	73%	73%
Executive	EXE	91%	84%	57%	52%	71%
Human Resources	HR	65%	67%	74%	67%	68%
Public Works & Services	PWS	63%	61%	64%	65%	63%
Finance	FIN	58%	63%	60%	56%	59%
Average %		76%	76%	77%	75%	76%

GNWT-Wide Overtime Audit
Lieu Time Hours Banked Above 75 Hours
April 1, 2012 to March 31, 2016

Schedule V

Department		Fiscal Year				Total
		2012-2013	2013-2014	2014-2015	2015-2016	
Energy & Natural Resources	ENR	420	513	720	1112	2,765
Justice	Justice	522	850	387	991	2,750
Public Works & Services	PWS	624	216	253	605	1,698
Education, Culture & Employment	ECE	495	327	257	407	1,486
Municipal & Community Affairs	MACA	434	342	311	304	1,391
Transportation	Trans	182	231	504	471	1,388
Executive	EXE	375	388	87	13	863
Health and Social Services	HSS	192	192	236	98	718
Legislature	LEG	104	233	159	96	592
Finance	FIN	61	40	247	245	593
Industry, Tourism and Investment	ITI	43	130	150	262	585
Aboriginal Affairs/Intergovernmental Relations	AAIR	163	109	52	10	334
Human Resources	HR	142	68	43	30	283
Lands	Lands	NA	NA	110	91	201
Total Hours Above 75 hour limit:		3,757	3,639	3,516	4,735	15,647

Total LTE Hours Banked over 4 year period:	221,381
Total Hours Above 75 hour limit:	15,647
% LTE banked above HRM perscribed limits:	7%

GNWT-Wide Overtime Audit
 Call Back Hours Banked (CBE)
 April 1, 2012 to March 31, 2016

Schedule VI

Department		Fiscal Year				Total
		2012-2013	2013-2014	2014-2015	2015-2016	
Transportation	Trans	608	413	311	278	1,610
Public Works & Services	PWS	547	404	490	144	1,585
Justice	Justice	77	177	190	440	884
Finance	FIN	0	0	261	278	539
Human Resources	HR	194	255	8	0	457
Energy & Natural Resources	ENR	224	88	64	57	433
Education, Culture & Employment	ECE	76	64	72	64	276
Industry, Tourism and Investment	ITI	140	0	0	0	140
Health and Social Services	HSS	9	3	12	18	42
Legislature	LEG	0	0	4	0	4
Total CBE Hours		1,875	1,404	1,412	1,279	5,970

GNWT-Wide Overtime Audit
April 1, 2012 to March 31, 2016

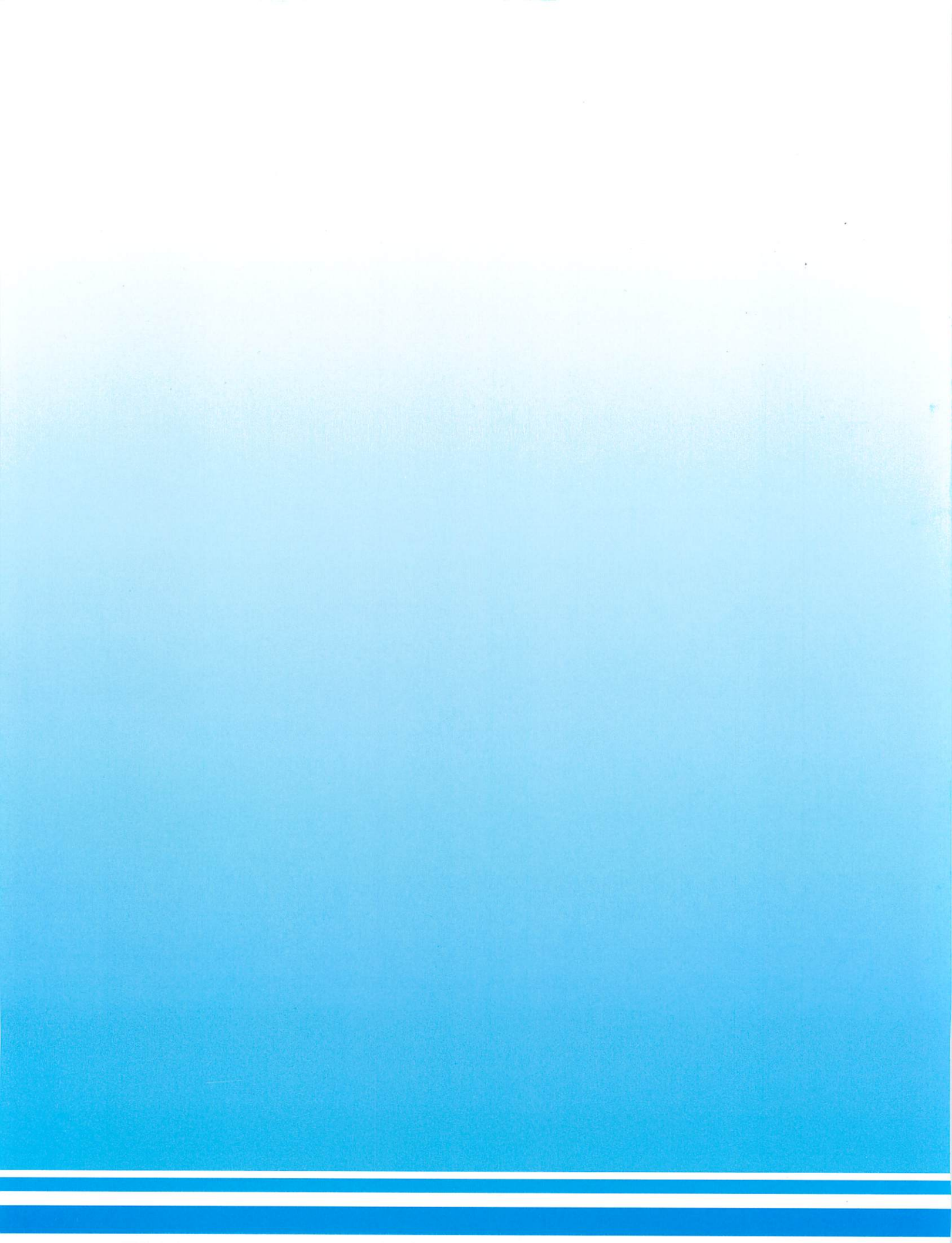
Schedule VII

Approvals of OT1/OT4/LTE Less than 1 Hour

Department		Fiscal Year				Total
		2012-2013	2013-2014	2014-2015	2015-2016	
Transportation	Trans	54	585	495	646	1,780
Justice	Justice	92	197	179	234	702
Finance	FIN	20	28	223	74	345
Public Works & Services	PWS	33	57	57	80	227
Education, Culture & Employment	ECE	22	NA	122	68	212
Human Resources	HR	41	85	8	24	158
Energy & Natural Resources	ENR	19	41	33	29	122
Lands	Lands	NA	NA	80	36	116
Health and Social Services	HSS	11	40	17	29	97
Municipal & Community Affairs	MACA	6	25	13	25	69
Industry, Tourism and Investment	ITI	2	12	22	18	54
Executive	EXE	14	28	3	3	48
Legislature	LEG	6	29	5	0	40
Aboriginal Affairs/Intergovernmental Relations	AAIR	6	1	8	5	20
Total OT1/OT4/LTE Approvals < 1 Hour		326	1,128	1,265	1,271	3,990

Approvals of OT1/OT4/LTE greater than 4 hours

Department		Fiscal Year				Total
		2012-2013	2013-2014	2014-2015	2015-2016	
Transportation	Trans	32	109	116	85	342
Public Works and Services	PWS	51	74	84	88	297
Justice	Justice	59	75	59	79	272
Energy and Natural Resources	ENR	25	60	57	44	186
Finance	FIN	5	58	66	25	154
Education, Culture and Employment	ECE	40	NA	65	36	141
Industry, Tourism and Investment	ITI	9	25	44	52	130
Executive	EXE	11	59	27	16	113
Health and Social Services	HSS	14	17	31	28	90
Lands	Lands	NA	NA	33	48	81
Municipal and Community Affairs	MACA	4	22	9	14	49
Human Resources	HR	4	12	5	21	42
Legislative	LEG	2	13	8	17	40
Aboriginal Affairs/Intergovernmental Relations	AAIR	13	5	4	4	26
Total OT1/OT4/LTE Approvals > 4 Hours		269	529	608	557	1,963





CONFIDENTIAL

November 29, 2021

File: 7820-30-GNWT-151-113

MR. WILLIAM MACKAY
CHAIR
INFORMATICS POLICY COUNCIL

**Audit Report: Corporate Informatics and Communication Technology Applications
Demographics Data Analysis**

Audit Period: As of March 31, 2021

A. SCOPE AND OBJECTIVES

The Audit Committee approved the assessment of demographic data retained in GNWT departments' Informatics and Communication Technology (ICT) applications. The project objective was to use the data analysis tool to determine whether the ICT application databases contained relevant, accurate, and complete client and employee information supporting fiscal responsibility, accountability, and transparency.

We conducted an in-depth data analysis of select ICT applications in four departments. This report identifies corporate issues beyond the scope of the individual department that could be best addressed by the Office of the Chief Information Officer (OCIO).

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

B. BACKGROUND

The GNWT Informatics Policy Council's Information Management Policy (Policy) guides GNWT departments to take a consistent approach to recorded information management. The Policy holds Deputy Ministers accountable for the management of recorded information in their respective departments. The OCIO, as the GNWT's senior authority for ICT, guides departments on policy implementation.

At the request of the OCIO, the Internal Audit Bureau (IAB) surveyed GNWT departments and identified 75 ICT applications containing demographic information such as name, address, date of birth, and Social Insurance Number. Some of the key attributes of ICT databases show:

Department	# of databases collecting personal information	# of databases with a legal framework to collect client data	# of databases interfacing with other GNWT databases	Documented process to collect, store and process client data	# of Databases that can export flat files	Databases containing SIN and/or Business Numbers
FIN	7	-	5	6	7	2
MACA	3	3	0	3	0	0
ECE	7	-	4	5	6	4
INF	13	-	4	10	9	2
HSS	6	-	3	2	6	2
JUS	14	12	6	10	13	9
ITI	9	9	4	-	8	2
ENR	11	11	4	-	9	1
LND	5	5	1	-	5	1
Total	75	40	31	36	63	23

Blank (-) = did not obtain information

C. SYNOPSIS

An in-depth data analysis of select ICT applications was performed to identify outstanding risks and provide recommendations to four departments: (**Appendix A refers**)

- Education Culture & Employment (ECE)
- Finance (FIN)
- Health & Social Services (HSS)
- Infrastructure (INF).

Departments recognized the importance of demographic information for delivering programs and services to the NWT residents and employees. Maintaining accurate and complete information was integral to GNWT's ability to provide reliable programs and services. Some of the databases we examined contained critical information to provide medical services, identification, authentication for cross-border use, and safe transportation of goods and people.

An error in demographic data, such as name and date of birth, might not be identified by the client or employee for an extended period, such as retirement or death. The impact of an error was significant, as was the effort required to correct it. Once correctly recorded, the demographic information was usually stable in the ICT applications requiring little change.

The OCIO can take the leadership role in providing strategic direction to departments in improving data integrity, allowing the generation of reliable information that could give insight to program managers for program delivery. OCIO involvement was required in:

1. Departmental ICT application Quality Assurance/Quality Control (QA) programs with support from tools such as data analytics, artificial intelligence, and robotics.
 - a. Typically, the QA internal controls adopted by departments were labour-intensive. The effectiveness of internal controls based on a manual review in the face of a large volume of transactions was problematic. All the departments agreed to establish a QA program to improve database integrity.
2. A GNWT wide data management framework to improve data conversion and data sanitization from legacy ICT applications for all departments.
 - a. Some databases did not have a clean conversion from the legacy database or have contaminated databases in subsequent updates. We were informed about a database where over 80% of the records were contaminated more than 15 years ago during conversion. The department has a manual workaround solution but no cohesive plan to address the contaminated database.

3. A common client registry as a foundation for the one-stop-shop for government services while considering data demographic standards and digital identity and program area legislation.
 - a. A range of data entries occurred due to lack of established standard and edit validation rules. ICT applications could not recognize the change in the operating environment, such as name spelled with symbols, use of single name only, etc. There was some level of consistency within each application but not across departments. A precondition of a government-wide database requires consistency across government applications.
4. A government service number that facilitates the coordination with Federal, Provincial, and Territorial jurisdictions.
 - a. There was an increased need for GNWT to interact at the pan-Canadian level. Our partners require that the information they provide will be protected and the information they receive has integrity.
5. The disposal of archived data in compliance with the Access to Information and Protection of Privacy Act (ATIPP).
 - a. Significant data was collected from NWT clients and GNWT employees that should not be obtained under the current ATIPP. Departments have stopped collecting such data to conform with ATIPP. A significant amount of archival data needs to be cleansed to meet ATIPP requirements.

D. ACKNOWLEDGEMENT

We want to thank OCIO staff for their assistance and co-operation throughout this project.



Stephanie Carter
Director, Internal Audit Bureau
Finance



CONFIDENTIAL

March 5, 2021

File: 7820-30-GNWT-151-113

MR. SANDY KALGUTKAR
DEPUTY MINISTER
FINANCE

Audit Report: ICT Demographics Data Analysis
Audit Period: As of November 30, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the assessment of demographic data retained in the GNWT department's Informatics and Communication Technology (ICT) applications.

The audit objective was to use the data analysis tool to determine whether the ICT application databases contained relevant, accurate, and complete client information supporting fiscal responsibility, accountability, and transparency.

This report identified issues specific to the Department of Finance (Finance). Some ICT issues beyond the control of Finance will be reported in a corporate report and forwarded to the Office of the Chief Information Officer (OCIO) for further action.

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

B. BACKGROUND

In 2018, the Internal Audit Bureau (IAB) identified 75 ICT applications in the GNWT containing demographic information including name, address, date of birth, and Social Insurance Number.

The GNWT Informatics Policy Council's Information Management Policy (Policy) guides the GNWT departments to take a consistent approach to recorded information management. The Policy holds the Deputy Ministers accountable for the management of recorded information in their respective departments. The OCIO, as the GNWT's senior authority for ICT, guides departments on policy implementation.

Finance had seven databases that contained demographic information. The System for Accountability and Management (SAM) and the Human Resource Information System (HRIS) support the GNWT's financial, procurement, human resource, and payroll functions. Collectively, they contained about:

- 30,000 records of SAM customers
- 40,000 records of SAM vendors
- 40,000 records of employees (HRIS).

C. OVERVIEW

The enterprise-wide use of SAM and HRIS was critical to support the delivery of GNWT programs and services. A small error in SAM or HRIS demographic data could adversely affect GNWT employees and NWT residents. Over 99% of SAM and HRIS demographic data complied with the requirements. The following data integrity areas require management attention (**Schedule I refers**):

- SAM data analysis showed:
 - The potential for payments being processed earlier than required.
 - Data entry and duplication errors compromising the integrity of the data; and
 - The retention of archived "legacy" data that may be non-compliant with the *Archives Act*.
- HRIS data analysis showed:
 - Data fields that were incomplete or inaccurate which could impact employee pay or benefits; and

- The collection and retention of potentially unnecessary information could be non-conformance with the *Access to Information and Protection of Privacy Act*.

The review showed that the likelihood of error in demographic data for SAM and HRIS was almost inevitable. Preventive controls, such as compliance with the documented process by all users, and the design of edit validation rules for the applications, would reduce the likelihood of error.

The impact of data entry varied depending on the error. In some cases, the impact was immediate, with a fair number of vendors getting early payment by being incorrectly classified as a northern vendor. In other cases, especially for GNWT employees, the impact may not be identified for years. Detective controls, such as the review of data entry, could identify errors early in the process and reduce the error's impact.

There was a delay in development management responses due to COVID-19. Management has developed risk mitigations plans to address the risks identified in the audit report.

D. ACKNOWLEDGEMENT

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



T. Bob Shahi
Director, Internal Audit Bureau
Finance

Observation 1: SAM Data Accuracy

Criteria:

- Recorded information used to conduct government business must be created and managed in a way that maintains its usefulness, authenticity, and reliability– *Management of Electronic Information Policy 6003.00.20*
- Departments manage recorded information in their custody consistent with this policy, the Archives Act, ATIPP, FAA, and all other GNWT legislation – *Recorded Information Management Policy*

Condition / Evidence

The data analysis to validate the accuracy of unique client identifiers within the SAM Vendor and Customer data tables identified the following:

Vendor Information

The Vendor data table contained 41,995 records. The details of the following exceptions were provided to the risk owner:

- 21,743 unique Vendor IDs were listed with an NT Address without 20-day payment terms – indicating that these vendors may qualify under the Business Incentive Policy (BIP).
- There were 1,274 unique Vendor IDs with 20-day payment terms; however, according to the Manager of BIP & Contract Registry, there were 1,210 BIP registered vendors. Data showed that 1,190 were listed with an NT Address while 84 had an outside NT Address.
- 158 records with unique Vendor IDs contained the same Name.
- 115 records with unique Vendor IDs contained a minor variation in the Name field (differences in punctuation, capitalization, spaces, or spelling, defined as “fuzzy analysis”).
- 109 records where the Vendor Location Description was missing.
- 32 records were missing the mandatory City or State.

Customer Information

Out of 28,851 records in the SAM Customer data table, 28,562 were identified as “Active,” and 289 were “Inactive.” The details of the following exceptions in the Active data were provided to the risk owner:

- 590 records with unique Customer IDs contained a minor variation in the Name field, identified through “fuzzy analysis.”
- 200 records with a unique Customer ID contained the same Name.
- 14 records with unique Names contained the same Customer ID.
- 25 records were missing the mandatory City, State, or Postal Code. Note: This analysis was only for CAN or USA addresses.
- Two records included “Do Not Use” in the Name or Address.

Risk/Consequence:	
<ul style="list-style-type: none"> Financial resources may be disbursed to incorrect, ineligible, or duplicate vendors or customers Service delays caused by missing client or vendor information may negatively affect the government's reputation Payment made before the due date may negatively impact the GNWT cash position Payment not made within BIP payment terms may negatively impact GNWT reputation 	<p>Risk Rating: High Likelihood: Almost Certain Impact: Moderate Risk Owner: Assistant Comptroller General, Finance Support:</p> <ul style="list-style-type: none"> Executive Director, FESS, Finance Executive Director, ERP, Finance
Recommendations:	
<p>To meet the objective that recorded demographic data supports fiscal responsibility, accountability, and transparency, we recommend that the Assistant Comptroller General or delegate:</p> <ol style="list-style-type: none"> Develop and implement a process in conjunction with the BIP & Contract Registry Team to maintain a current and accurate BIP-vendor listing in SAM. Implement a Quality Assurance/Quality Control process to detect data entry errors for corrections. In coordination with Archives, develop an approved retention and disposal schedule of SAM records to discharge responsibility under the FAA. 	
Management Response:	Timeline:
1. Management will develop and implement a process in conjunction with BIP that will include a current review and will ensure that the vendor data is accurate on a go-forward basis. The process will also highlight exceptions that should be incorporated when a user is accessing this data (e.g. individuals are vendors who will not be BIPed who will have an NT address)	September 2021
2. Management will conduct a review of the results of the audit and confirm any exceptions, as well as develop and implement a quality assurance/control process in conjunction with the accounting system's ability.	December 2021
3. In conjunction with managements responses to number 2 above, management will work with the SAM team to address inactive accounts in SAM	December 2021

Observation 2: HRIS Data Accuracy and Completeness

Criteria:

- Reasonable effort must be made to ensure personal information used to make a decision affecting an individual is accurate and complete – *ATIPP 44 (a)*
- Recorded information used to conduct government business must be created and managed in a way that maintains its usefulness, authenticity, and reliability– *Management of Electronic Information Policy 6003.00.20*
- “Integrity” of information refers to information being complete and accurate with no unauthorized alterations – *Electronic Information Security Policy*
- Recorded information support decision-making and maintain government accountability to the public for its actions – *Recorded Information Management Policy*

Condition / Evidence

The HRIS database contained approximately 40,000 records with multiple fields containing demographic data. We conducted data analysis to validate the accuracy of unique client identifiers and the completeness of demographic data. We confirmed the validity of some data fields, such as National ID (SIN). Data analysis also showed that information was complete for Name, Last Name, First Name, SIN, Gender, Marital Status, and Date of Birth fields. The preliminary data analysis used all the records, showing that a large amount of data in the HRIS system was incomplete/incorrect. Subsequently, we limited our data analysis to the 7,108 “Active” records. We noted the following exceptions in the Active data:

Data Accuracy The details of the following exceptions were provided to the risk owner:

1. Two records contained the same National_ID (SIN) and Name, with different Employee IDs.
2. One record contained “Do Not Use” in the Address1 field.
3. Ten records had a Name Prefix that did not correspond with the designated Sex (e.g. Mr. = F).
4. Potential anomalies in Date of Birth:
 - a. 23 records where Date of Birth is before 1940 (employee is over 80 years old)
 - b. One record where the Date of Birth is 1/7/2016 (employee is 3 years old).
5. 116 records with “Estate of” in the Name field without a corresponding Date of Death.
6. 5,996 records contained Birth Place, Birth State, or Birth Country.

Data Completeness–The details of the following exceptions were provided to the risk owner:

1. Blank records in the mandatory Address fields as follows:
 - a. Six records without Address1, City, State, Postal Code, or Country
 - b. Seven additional records were missing Postal Code.
2. 253 records without a Phone Number (preferred data).
3. 2,667 records without a Name Prefix (preferred data).

Risk/Consequence:

- The GNWT having inaccurate employee information may impact payroll or employee benefits
- Service delays caused by missing employee information may affect the government’s reputation
- Financial resources may be disbursed to incorrect or ineligible personnel
- Management may be reporting inaccurate employee information.

Risk Rating: High
Likelihood: Almost Certain
Impact: Moderate
Risk Owner: Deputy Secretary of Human Resources, Finance Support:

- Executive Director, FESS, Finance
- Executive Director, Enterprise Resource Planning, Finance

Recommendations:

To meet the reporting requirements of the Public Service Act (to report complete and accurate information on GNWT employees), we recommend that the Deputy Secretary of Human Resources or delegate:

1. Document and communicate direction for mandatory versus non-mandatory fields in HRIS.
2. In coordination with the Access and Privacy Office, conduct a Privacy Impact Assessment on data collected and retained in the HRIS database.
3. Implement a Quality Assurance/Quality Control process to detect data entry errors for corrections.
4. In coordination with Archives, develop an approved retention and disposal schedule of personnel records (electronic and recorded).

Management Response:	Timeline:
1. Clarity and consistency of mandatory vs. non-mandatory fields in HRIS will be documented.	June 2021
2. Engage with the OCIO and the Access and Privacy Office for a Privacy Impact Assessment on HRIS data to ensure compliance with ATIPP.	August 2021
3. Review the current queries run by FESS regularly to identify errors to determine effectiveness and value add.	December 2021
4. Engage the HRIS team to determine how historical electronic records should be managed to comply with Archives Act.	September 2021

**GNWT Wide Procure to Pay Process
Operational Audit Report**

Internal Audit Bureau

July 2019

THIS PAGE INTENTIONALLY LEFT BLANK



CONFIDENTIAL

July 4, 2019

File: 7820-20-GNWT-151-137

MR. DAVID STEWART
CHAIR
DEPUTY MINISTER SHARED SERVICES

Audit Report: Procure to Pay Process
Audit Period: As of March 31, 2019

A. SCOPE AND OBJECTIVES

The Audit Committee approved the operational audit of Government of Northwest Territories (GNWT) Procure to Pay Process (P2P). The audit covered the full cycle of procurement started by departmental to final payment to vendors for goods and services.

B. BACKGROUND

Annually, the GNWT spends over \$400 million for procurement of goods and services. The Financial Administration Act, the Financial Administration Manual, and the Government Contract Regulations form the legal framework for procurement. The GNWT has also established two shared services centers to support departments in the procurement process:

- Procurement Shared Services in the Department of Infrastructure (PSS)
- Financial and Employees Shared Services in the Department of Finance (FESS).

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 attached audit report by the contractor, "*Procure to Payment Process Audit*" provides the details on the scope, objective, background and 15 high-risk observations with recommendations (**Schedule I refers**). The management responses to these recommendations have been incorporated in the attached report.

Nine additional observations with lower risks were provided for management consideration (**Appendix L refers**). These observations provided information on the improvement of the P2P process that could be implementation at management discretion.

The overall risk assessment of P2P was rated as high-risk, indicating a need for capacity at a managed level to defuse the risk. Some of the attributes of managed capacity include:

- Key performance indicators and monitoring techniques to measure success
- Greater reliance on prevention versus detection
- Strong self-assessment of operating effectiveness by process owners
- Chain of accountability.

The P2P was working. The foundation for P2P was a solid legal framework, and many of the processes were documented.

Work had already started to improve the P2P process capacity, such as the identification of key performance indicators for FESS and PSS. Other areas for consideration presented in the report include clarification of roles and responsibilities and monitored for compliance.

We will follow-up on the management actions in addressing the risks identified in the 15 observations in about six months.

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

THIS PAGE INTENTIONALLY LEFT BLANK

SCHEDULE I

**GNWT WIDE - PROCURE TO PAYMENT
PROCESS AUDIT REPORT**

CONDUCTED BY CROWE MACKAY LLP

THIS PAGE INTENTIONALLY LEFT BLANK



Date: July 3, 2019

To: T. Bob Shahi, Director, Internal Audit Bureau; Government of the Northwest Territories

From: Edward Olson, Practice Leader, Advisory Services, Crowe MacKay LLP

Re: Procure to Payment Process Audit

EXECUTIVE SUMMARY

Background

The Internal Audit Bureau (IAB) of the Government of the Northwest Territories (GNWT) issued a request for proposal for an operational audit of the Procure to Payment Cycle (P2P). P2P encompasses each GNWT department's approach to the procurement of goods and services from requisition to final payment and file closure.

In conjunction with the IAB, a work plan and determination of areas of focus were carried out and detailed in the planning memo dated March 12, 2019. The work plan included a review of the full P2P cycle, including FESS, PSS and the 11 Departments. The scope of this operational audit excluded the Northwest Territories Housing Corporation (NWT HC) and the 9 public agencies. Audit work focused on evaluating high-level policies, procedures, control frameworks and control processes which have been designed and implemented to ensure fairness, openness and transparency in procurement activities while simultaneously allowing flexibility to meet individual business needs.

Objectives

The objectives of this operational audit were to provide independent assessment and assurance to senior management regarding the following:

1. Ensure that the role and responsibilities of Procurement Shared Services (PSS), Financial and Employee Shared Services (FESS), departments and vendors are well defined for the efficient and effective use of GNWT resources.
2. Assess whether the framework used by PSS and FESS for continuous improvement as well as providing advice and direction to departments is aligned to publically accepted standards for shared services in similar sized jurisdictions.
3. Determine whether the processes within PSS and FESS are efficient, effective and supported by:
 - a. Continuous results monitoring;
 - b. Results reporting to meet the Shared Services Agreement Requirements; and
 - c. Results reporting to meet Financial Management Board (FMB) requirements for fiscal responsibility, transparency, and accountability.
4. Determine if the interface of PSS and FESS with departments, vendors and other stakeholders are efficient and effective to avoid duplication of effort.
5. Determine if the interface of PSS and FESS with departments, vendors and other stakeholders are efficient and effective to avoid duplication of effort.

Scope

The scope of the audit included examining P2P activities encompassing the procurement, contracting and payment frameworks established and effective for the 2018-2019 fiscal year which included examining procurement and payment documents and contracts issued during that same period. Substantive testing completed through data analytics covered the period from April 1, 2018 to January 31, 2019. The fieldwork for the audit was conducted from February 26 to April 5, 2019.

Conclusion

The results of the operational audit indicate continued confusion between the roles and responsibilities of PSS and FESS as compared to that of each department. Clarity of these roles and responsibilities are imperative to meet expectations of efficiency and effectiveness. Where roles and responsibilities are clear, compliance monitoring is weak for enforcing defined expectations.

Overall observations indicate that there is currently a strong base of specific policies and procedures within FESS (outlining specific steps for FESS processes such as processing payments, dealing with stop payments, and foreign currency payments) and PSS (outlining specific steps for PSS processes including how to deal with different types of contracts: sole source, request for proposal, issuing change orders, and electronic filing in SAM). Higher level guidance is also in place within legislation, the Financial Administration Manual (FAM), Service Partnership Agreements and the Procurement Guidelines for P2P activities. Although there is a strong base of policies and procedures, issues have been noted regarding compliance and monitoring of compliance with policy, challenge with sufficiency of training, and insufficient technological capabilities to support effective contract management.

The conclusion for each audit objective is presented below.

Objective 1:	Risk: Efficiency and effectiveness erosion is apparent with the following:
Description: Ensure that the role and responsibilities of PSS, FESS, departments and vendors are well defined for the efficient and effective use of GNWT resources.	<p>Roles and responsibilities are unclear and/or are inconsistently applied bringing confusion between the departments and each shared service as to specific processes to be performed and who is responsible.</p> <p>Training is not set by role or authority level, is not consistently applied across all departments, and is not monitored to ensure all critical roles have completed necessary training modules.</p>

Objective 2:	Risk: Expectations of value to be derived from successful implementation of a shared service model is not being attained for greater efficiency, improved productivity, and being a catalyst for business process change:
Description: Assess whether the framework used by PSS and FESS for continuous improvement as well as providing advice and direction to departments is aligned to publically accepted standards for shared services in similar sized jurisdictions.	<p>FESS is perceived by departments as solely a transactional body and not a provider of advice and/or assistance.</p> <p>Departments do not perceive consistency in service levels of PSS across all regional areas.</p> <p>Full operation as a shared service model is not achieved with some responsibilities still being delegated to departments (i.e. contract management, invoice processing).</p> <p>Inadequate monitoring of GNWT credit card transactions as FESS no longer conducting spot checks of departmental activities.</p>

	SAM framework for PSS is lacking a repository for creation and storage of standardized templates which leads to inefficiencies and increased error rates.
	PSS observations on contract files are not always documented and included with the respective file reviewed.
Objective 3:	Risk: Processes have been established but are not completely implemented to monitor results and report on achievement of operational requirements:
Description: Determine whether the processes within PSS and FESS are efficient, effective and supported by continuous results monitoring and results reporting.	Technology functionality is restricted preventing PSS from efficiently meeting its mandate. Modules within SAM are enabled but are ineffective in meeting operational requirements for contract management.
	A post-implementation review by a third party was not conducted to ensure PeopleSoft 2.0 met PSS, FESS and departmental objectives or enhanced effectiveness and efficiency of their operations.
	Time is spent attempting to work with the SAM system as configured and not on maximizing its value to monitor operations.
	There are duplicate names for both suppliers and vendors in SAM which leads to lack of efficiency for all aspects of the P2P cycle.
Objective 4:	Risk: The current interface has not removed the risk of duplication of effort or the full realization of effectiveness and efficiency of operations:
Description: Determine if the interface of PSS and FESS with departments, vendors and other stakeholders are efficient and effective to avoid duplication of effort.	Procurement Guidelines and the Shared Services Agreement contradict roles and responsibilities.
	Departments undertaking processes that should be performed by a shared service (i.e. invoice payment and contract preparation).
	Contract management responsibilities are not effective or consistently applied, checklists are not being used, and records are not being stored according to guidance.
	Sole source assignments and the use of change orders associated with these contracts are being used to avoid competitive bid/tender process.
Objective 5:	Risk: Current processes are not in compliance with legislation, policy and procedures to safeguard GNWT assets:
Description: Assess whether the processes used by PSS, FESS and Departments are in compliance with legislation, policy and procedures to safeguard GNWT assets.	Departments are able to adjust committed funds after contracts have been established and finalized in contradiction of the Financial Administration Act (FAA).
	Contract file maintenance is not in accordance with records management guidelines.
	Contract files maintained by departments are missing necessary documentation.

Objective 5:	Risk: Current processes are not in compliance with legislation, policy and procedures to safeguard GNWT assets:
	Formal vendor assessments are not performed to ensure compliance with contract terms.
	Payment processing times are not in accordance with FAM
	Invoice approval controls may be missing as a result of changes to expenditure authorities when electronic approvals were introduced

The full report has been constructed based on the full business cycle of P2P. A review of shared services is followed by training and awareness, continues through to initiation and authorization of procurement activities, followed by contract management and ultimately final payment to vendors. An analysis has also been made to assess shared services.

Table of Contents

SCOPE AND OBJECTIVES.....	6
BACKGROUND	7
FINDINGS & OBSERVATIONS	8
A. SHARED SERVICES	9
B. TRAINING & AWARENESS.....	17
C. PROCUREMENT	19
D. CONTRACT MANAGEMENT	24
E. PAYMENT	29
APPENDIX A: ADDITIONAL BACKGROUND DETAILS.....	37
APPENDIX B: FAM ROLES & RESPONSIBILITIES	39
APPENDIX C: SERVICE PARTNERSHIP AGREEMENTS	42
APPENDIX D: ESSENTIAL CONCEPTS (FAA AND GCR)	43
APPENDIX E: DEPARTMENTAL CONTRACTING RISK ASSESSMENT	44
APPENDIX F: DEPARTMENT RISK CRITERIA.....	46
APPENDIX G: PSS & FESS APPROACH.....	48
APPENDIX H: VALUES AND GUIDING PRINCIPLES OF PUBLIC PROCUREMENT	49
APPENDIX I: INTERNAL CONTROL CAPACITY MODEL	51
APPENDIX J: AUDIT RISK ASSESSMENT HEAT MAP	54
APPENDIX K: CONTRACTS FOR FOLLOW-UP FROM OBSERVATION 8	57
APPENDIX L: GENERAL OBSERVATIONS FOR MANAGEMENT CONSIDERATION	58

SCOPE AND OBJECTIVES

The Internal Audit Bureau (IAB) of the Government of the Northwest Territories (GNWT) issued a request for proposal for an operational audit of the Procure to Payment Cycle (P2P). P2P encompasses each GNWT department's approach to the procurement of goods and services from requisition to final payment and file closure. Crowe MacKay LLP (Crowe) coordinated all work related to this operational audit directly under the supervision of the Director, Internal Audit Bureau. The following objectives were established by the IAB to guide audit activities from planning through fieldwork and ultimately to final reporting:

- **Objective 1:** Ensure that the role and responsibilities of Procurement Shared Services (PSS), Financial and Employee Shared Services (FESS), departments and vendors are well defined for the efficient and effective use of GNWT resources.
- **Objective 2:** Assess whether the framework used by PSS and FESS for continuous improvement as well as providing advice and direction to departments is aligned to publically accepted standards for shared services in similar sized jurisdictions.
- **Objective 3:** Determine whether the processes within PSS and FESS are efficient, effective and supported by:
 - Continuous results monitoring;
 - Results reporting to meet the Shared Service Agreement Requirements; and
 - Results reporting to meet Financial Management Board (FMB) requirements for fiscal responsibility, transparency, and accountability.
- **Objective 4:** Determine if the interface of PSS and FESS with departments, vendors and other stakeholders are efficient and effective to avoid duplication of effort.
- **Objective 5:** Assess whether the processes used by PSS, FESS and Departments is in compliance with legislation, policy and procedures to safeguard GNWT assets.

Crowe conducted initial meetings with the IAB as well as with representatives from PSS and FESS to identify the current state of activities and areas of concern in the P2P cycle. This information gathering was conducted as part of the planning process and prior to the start of fieldwork. Feedback received was utilized in assessing risk within the P2P cycle as well as to suitably plan audit procedures for this engagement.

Fieldwork was undertaken utilizing the International Standards for the Professional Practice of Internal Auditing as defined by the Institute of Internal Auditors. This ensured a risk-based internal audit plan which applied a methodology that links internal audit procedures to an organization's overall risk management framework.

This audit encompassed each of the 11 departments, PSS as well as FESS. Policies, procedures and internal controls designed and implemented regarding the P2P cycle, and in alignment with the Financial Administration Act (FAA) and Financial Administration Manual (FAM) and related guidelines and policies, were the basis for this operational audit. Due to the breadth of audit coverage, the primary focus remained on firstly evaluating the design of internal controls and secondly on the operational effectiveness of these same controls.

The scope of this operational audit excluded the Northwest Territories Housing Corporation (NWT HC) and the 9 public agencies. Audit work was related directly to the objectives noted above and on high-level policies, procedures, control frameworks and control processes. Audit procedures did not include transaction level testing except for the departments chosen for additional focus as specified in the "Approach" sections later in this report.

Although an understanding of the SAM modules in use for procurement activities was obtained, and some suggestions for improvement have been identified within this report, this audit did not include procedures to specifically assess the SAM system. SAM was only considered in relation to the processes and controls assessed within the P2P cycle and their support of those processes and/or controls.

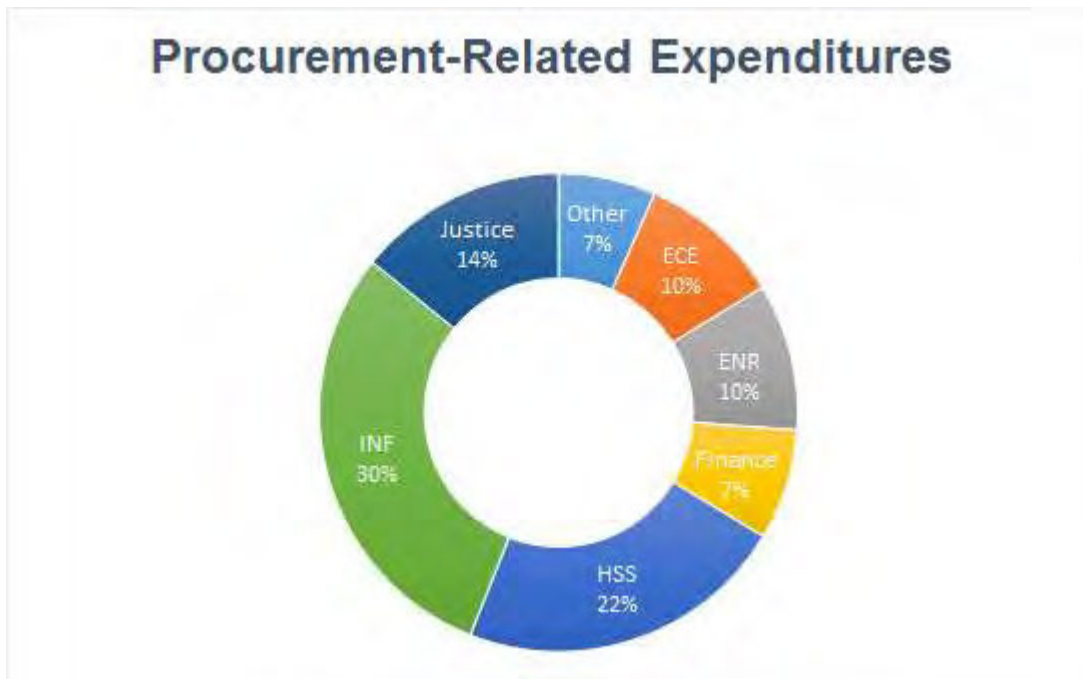
BACKGROUND

Quantitative analyses of departmental expenditures have been reported using the full fiscal period for 2017-2018 to provide an overview of procurement activity. Due to the timing of fieldwork, reporting on the 2018-2019 fiscal period was based on actual plus estimates. See the following table:

Department	2018-2019 Revised Estimates (\$000's)	2017-2018 Actual (\$000's)
Education, Culture & Employment (ECE)	327,058	322,912
Environment, and Natural Resources (ENR)	88,059	95,463
Executive and Indigenous Affairs (EIA)	21,869	18,941
Finance (FIN)	252,543	247,230
Health and Social Services (HSS)	463,773	445,642
Industry, Tourism and Investment (ITI)	57,283	58,314
Infrastructure (INF)	245,492	243,997
Justice (JUS)	124,959	123,683
Lands (Lands)	21,348	18,213
Legislative Assembly (Leg)	20,849	18,376
Municipal and Community Affairs (MACA)	107,819	106,177
Total Expenditures	1,731,052	1,698,948
Less Non Procurement-related Expenditures ¹	(1,326,318)	(1,297,010)
Total Procurement-related Expenditures	404,734	401,938

Note 1: Includes amortization, compensation and benefits, grants, contributions, transfers, chargebacks, interest, loss on sale of assets, and valuation allowances.

Total procurement-related expenditures for the 2017-2018 fiscal period have been delineated by department in the following chart. Identifying the concentration of procurement activities by department provides a solid risk-based starting point from which audit fieldwork was planned. The chart below provides department names for those with the highest concentration of procurement activities.



Roles and responsibilities of departments, PSS and FESS are outlined in a number of policies and procedures as well as within legislation. Please see the following appendices include pertinent information utilized in this audit:

- Appendix B Summary of roles and responsibilities per FAM
- Appendix C Summary of roles and responsibilities in the Service Partnership Agreements
- Appendix D Overarching principles of the FAA and Government Contract Regulations (GCR)
- Appendix G Approach to PSS and FESS testing

Procurement-related expenditures for the 2017-2018 fiscal period were \$401,938,000. Per the “Government of the Northwest Territories Contract for Goods Over \$25,000 or Services/Construction over \$25,000 Report for the April 1, 2017 to March 31, 2018 Reporting Period”, expenditures for which contracts were used totaled \$325,950,562 or 81% of total procurement-related activities. The significance of this value to total procurement activity was a primary driver for substantive testing to be performed in relation to these contracts at both PSS and in the respective departments. In addition, risk profiling was completed on each department to further hone the focus for substantive testing (see Departmental Contracting Risk Assessment in Appendix E).

Due to recent changes in system upgrades in Q1 2018, Crowe conducted substantive and analytical testing on data for the period April 1, 2018 through to January 31, 2019. The data selected for testing would then reflect the updated processes and controls implemented by management and whether risks within the P2P cycle have been adequately identified and mitigated. Testing prior to the upgrade date would provide limited value to the recommendations within this report.

Non-contract expenditures exist and represent transactions less than \$10,000 which are paid through GNWT credit card, in addition to services less than \$10,000. Focus on these transactions was undertaken through data analytics versus relying on sampling and substantive testing individual transactions.

FINDINGS & OBSERVATIONS

Findings and observations have been categorized in accordance with the flow of the P2P cycle. These categories begin with training and awareness, continue through initiation and authorization of

procurement activities, followed by contract management and ultimately ending with final payment to vendors. This audit assessed each of the areas for both design as well as operational effectiveness of internal controls. Ratings within this report have been provided using the Internal Audit Bureau's internal control capacity model (see Appendix I) and audit risk assessment heat map in (see Appendix J). Higher risk findings and observations are included in the body of this report. General observations for management consideration have been included in Appendix L.

A. SHARED SERVICES

Shared services are quite different in nature to centralization of operational functions such as transactions; it is important to have an understanding of the main difference in structure when analyzing the effectiveness of a shared service such as PSS or FESS. Some of the main differences have been outlined in the following table:

Attribute	Centralization	Shared Service
Customers	Viewed as end users of service.	Viewed as clients who have input and value.
Governance	Varies and is likely to have multiple areas of input from an oversight perspective as the ownership lies elsewhere.	Managed as its own unit, with strategy, oversight planning, etc. by senior management of the shared service.
Main Focus	Transaction cost and efficiency.	Service excellence, high performance, continuous improvement, along with cost and efficiency.
Service Responsibility	Central oversight entity.	Shared between service and clients as stated in service level agreements.
Accountability	Accountable to overall entity.	Accountable to clients (departments) directly.
Service Management	Varied.	Service level agreements, key performance indicators, and performance reporting.
Performance Monitoring	Specific to cost and efficiency measures.	Continuous and always looking for improvement.

During the audit an assessment was made of PSS and FESS with regards to the sections noted above, both from an operational perspective as well as from the perspective of each entity's role as a service provider. Our evaluation is noted below.

Client service and provision of expertise and advice are essential differences between a shared service model and that of a centralized operations approach. Both FESS and PSS have a Service Partnership Agreement in place with the departments which outlines high level goals of the shared service entity. This includes the underlying service principles, service responsibility matrix, and related service standards. While the principles have already been established, the direction for delivery of these principles requires additional specificity for operations both within the shared services as well as within their interactions with departments.

Shared Services – Environmental Analysis

As part of the work performed, we considered other organizations/entities to determine how they approach shared services, if at all. Three entities were contacted to review their processes and procedures related to their P2P cycle. Results of these discussions are as follows:

Government of British Columbia

Shared Service Model	Department	Technology/Tools
<ul style="list-style-type: none"> • Creation of procurement policies and procedures • Assist with guidance when requested by departments • Create SOA's for standardized pan-governmental purchases • Negotiates for all departments on standard travel expenses and rates (i.e. hotels, rental cars, airfare) • Processes competitive bids through online website "BC Bid" • Creates and provides templates and forms • Provide training as/when needed 	<ul style="list-style-type: none"> • Office of the Controller General manages the Vendor List • All invoices received and processed by individual departments • Departments review all competitive bid responses received and make final decision 	<ul style="list-style-type: none"> • No contract management module within Oracle utilized • Departments make use of Excel to track contracts • Corporate Accounting System (CAS) utilized to match PR/PO/Invoice prior to payment • Transaction approvals in CAS

Note: The government is currently undertaking a full review of their P2P cycle for improvements as well as new technology to support necessary activities. Consideration is currently being given to having a centralized contract management module.

Government of Alberta

Shared Service Model	Department	Technology/Tools
<ul style="list-style-type: none"> • Creation of procurement policies and procedures • Assist with guidance when requested by departments • Processes competitive bids through online website "Alberta Purchasing Connection" • Creates and provides templates and forms • Provide training as/when needed 	<ul style="list-style-type: none"> • Autonomous to contract for goods/services as/when needed • All invoices received and processed by individual departments • Departments review all competitive bid responses received and make final decision 	<ul style="list-style-type: none"> • IMAGIS and not Oracle used • Transaction approvals in IMAGIS

Note: The government is in the process of replacing IMAGIS. A decision as to solution/direction has yet to be made as at the time of this report.

City of Calgary

Shared Service Model	Department	Technology/Tools
<ul style="list-style-type: none"> • Creation of procurement policies and procedures • Assist with guidance when requested by departments • Processes competitive bids through online website "Merx" 	<ul style="list-style-type: none"> • Autonomous to contract goods/services as/when needed • All invoices sent to Finance for processing • Departments must review and approve invoices in 	<ul style="list-style-type: none"> • In-house written database for contract management • Database interfaces with PeopleSoft • PeopleSoft used to match PR/PO/invoice prior to payment

Shared Service Model	Department	Technology/Tools
Calgary” or “Alberta Purchasing Connection” <ul style="list-style-type: none"> Creates and provides templates and forms Provide training as/when needed 	PeopleSoft before Finance can authorize payment	<ul style="list-style-type: none"> Transaction approvals in PeopleSoft

Of note in the various environments considered for their treatment of shared services and tools employed in the P2P cycle, is that shared services are in place to support the relatively autonomous departments. In contrast, the GNWT has moved to a more centralized approach of embracing shared services but has not fully passed authority to PSS or FESS which is creating confusion between the roles of these shared services and the departments. Consideration should be given to fully implementing a shared service model or reverting back to departments having their own autonomy.

Lastly, technology solutions are varied by entity. Two of the three entities are conducting a review of their technology platforms in order to adequately address their P2P cycle, including contract management. The City of Calgary has solved their contract management needs by developing their own in house application. GNWT has options through PeopleSoft for contract management which are still not functional. Consideration should be given as to whether these can be adequately employed or whether other solutions should be evaluated (outlined more in Observation 3).

FESS Analysis

Through interviews with FESS management as well as review of policy and procedure documents, it was clear that there are clear and concise processes in place for this shared service area. Recent changes to the DIIMS workflow has enabled management to conduct real-time monitoring of payment processing on a daily basis. This enables timely feedback for ongoing FESS staff performance in meeting departmental needs.

While feedback has been primarily positive regarding FESS’ role and performance in the P2P cycle, some concern was raised by departments that FESS is only a transaction-based function and is lacking in the services side of their role as a shared service. Specific examples related to the ability of FESS to address vendor queries as opposed to sending these queries back to the individual departments to address. Our interview with FESS management confirmed their awareness of this issue and that it will be evaluated for an effective solution.

In addition, departments have concern regarding the timing of payment processing. As noted in the data analysis section of this report, this has been previously identified as an issue by FESS and that some suggestions have been made to correct the issue. Full resolution of this has yet to be achieved. Lastly, departments are also concerned with the time required by FESS to setup new vendors.

Observation 1

FESS is not viewed by departments as a service provider, rather as a transactional body only.

Interviews with departments found their opinion of FESS is that they are well respected in terms of transactional capability. However, complaints were made that the departments want more than just processing of invoices; they are looking for additional support as expected within a true shared service model. At present, departments do not feel comfortable that they can contact FESS to assist with anything other than pure transactional query support.

Risk Profile:

Risk Rating	High
Risk Impact	The true value of the shared service model is eroded when perceived service levels do not match with departmental expectations; lost

	confidence results in inefficiencies as departments begin taking on more work ultimately intended for the shared service entity.
Risk Responsibility	DM Shared Services Committee
Risk Mitigation Support	FESS, Comptroller General, Departments

Recommendations:

We recommend that:

- a) A review be performed by FESS management, with input from the departments, to clarify areas where departments would like to receive additional service and assistance. Communication with vendors was raised, but there are likely other areas of service that could also be addressed.
- b) FESS work with staff to increase understanding of their service role; this could include enhanced training to ensure staff are employed with the knowledge and tools to meet departmental needs.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. The Office of the Comptroller General has four divisions that work to provide client support. FESS's role is to provide training and support related to only the transactional processing portion. Additional support on training and policy interpretation are provided by other divisions which are well understood by clients. The Office of the Comptroller General will do a survey of client departments on an annual basis to identify any service gaps.	March 2020
	b. FESS will continue to provide training to clients for transactional processing portion. FESS staff will be trained to redirect the client to other areas for policy and process improvement services	Ongoing

Observation 2

Spot checks are no longer performed by FESS on departmental credit card transactions.

FESS had historically conducted spot audits on GNWT credit card transactions. During this audit, it was confirmed that FESS is no longer performing this monitoring control. FESS management indicated the current staffing complement does not allow for these monitoring procedures to be completed. Additional staff would be required if requested of FESS.

Risk Profile:

Risk Rating	Medium-High
Risk Impact	Lack of monitoring of credit card transactions could result in fraud, theft or intent by the credit card user to by-pass transactional authority limits for procurement activity.
Risk Responsibility	Comptroller General
Risk Mitigation Support	Departments, Executive Director, FESS

Recommendations:

We recommend that:

- a) A review be performed by FESS management, with input from departments, to assess whether the risk in credit card transactions is sufficiently monitored through another departmental control. If monitoring is not being sufficiently carried out, the decision needs to be made as to whether the department or FESS will re-implement this control.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. FESS will be conducting spot audits on GNWT credit card transactions	Fall 2019

PSS Analysis

Results of interviews conducted revealed that PSS is effectively processing contracts in compliance with Procurement Guidelines. Departments consistently provided positive feedback in relation to most PSS activities, including their ability to ask and receive answers from PSS related to contract and vendor questions including options for, and receipt of, training.

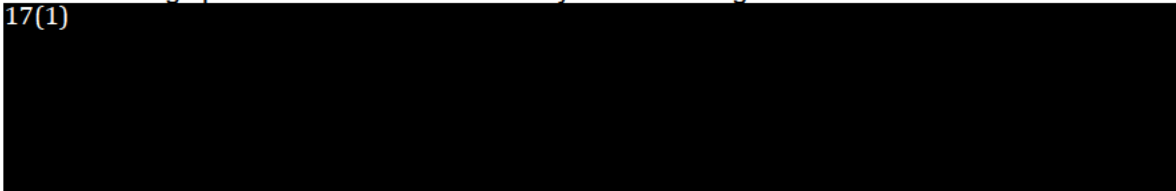
Feedback from PSS revealed inefficiencies in delivering on the roles they have been assigned as a shared service for departments. There are concerns with technical issues that have been experienced with historic as well as the current PeopleSoft 9.2 upgrade. Some of the most significant risk issues are outlined below.

Observation 3

Contract module is not being used due to problems with functionality in SAM.

The contract module is not being used by PSS staff for contracts as it is not fully functional. A workaround is being employed to leverage the functionality of the purchase order module. Employing technology for a purpose not originally intended increases risk to GNWT related to insufficient internal controls, insufficient access controls, as well as exposure to accuracy of data.

Some of these significant risks related to incorrect module utilization are as follows:

1. From this module the information no longer has continuity within the P2P cycle from requisition to purchase order. This increases the risk of error as numbers change in the system from the requisition, to contract, to PO. There is higher risk of data loss, or unexpected errors. For example, during testing it was noted that a contract was put through as a requisition for \$80,600, but the PO was put through for \$806,000 and then approved at this amount. System controls should prevent this type of error from occurring.
2. The use of the incorrect module results in an inefficient use of resources as this system was not designed to provide the functionality that is needed for appropriate contract management. PSS staff must manually copy, paste and input requisition data into the purchase order module which is an inefficient use of GNWT resources. Procedures which previously took PSS staff 20 minutes are now taking up to 1.5 hours. This inefficiency is a waste of government resources.
3. 17(1) 
4. Data produced from the SAM system relating to contracts will be incorrect if errors take place in data entry, and when commitment amounts are adjusted and moved. It was noted during file reviews at the department level that many contract managers (37%) are not comfortable working with and/or relying on SAM data and are tracking items in Excel. This suggests that the confidence in the SAM system is lacking, and is resulting in inefficiencies of data management.

Risk Profile:

Risk Rating	Very High
Risk Impact	Use of an incorrect SAM module has resulted in non-compliance with the FAA, very inefficient contract management processing; greatly increased risk of human error due to multiple entry points and lack of data continuity, and potentially incorrect reports being provided to the public.
Risk Responsibility	DM Shared Services Committee
Risk Mitigation Support	PSS, SAM Team, Comptroller General

Recommendations:

We recommend that:

- a) The contract module be brought to full functionality. Once functional, discontinue use of the purchase order module as currently utilized.
- b) An independent validation be conducted of functionality to ensure the module is operating effectively and efficiently, appropriate controls are operational, and contract data is complete and accurate.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. The contracting module is working as designed. Some of the workarounds were designed to accommodate the customize the ERP. The Office of the Comptroller General continues to engage PSS in using all the tools for process improvement. Current work of merging Health Authorities is the top priority for ERPS. Once that project is concluded, an assessment will be made, in consultation with the Office of the CIO, on eProcurement and other GNWT initiatives. The focus will be to leverage our existing investment in ERP and minimize customization, including the contracting module.	March 31, 2020
	b. The Office of the Auditor General audited the modules upon implementation and continues to assess system controls to ensure that information within the modules can be relied upon. The need for additional assurance will be considered if the risk profile of the project changes.	March 31, 2020

Observation 4

Contracting Templates within the SAM system are not adequate for the needs of PSS.

Templates relating to procurement processes that are available within SAM require formatting after being accessed for use. SAM only contains some templates with the remaining maintained in separate locations. There is no easily accessible library of current contracts for staff to access and make use of. This was confirmed during re-performance by audit staff of processes followed by PSS staff and the restrictions on templates/forms available. Contracts were noted as being mislabeled and would have to be edited prior to final use. This increases the likelihood that an incorrect form may be used due to lack of consistency in documentation which should be required for complex contracting processes.

Risk Profile:

Risk Rating	High
Risk Impact	Inconsistent contract management tools and templates; inefficient process in requiring standardized templates to require updating at each use.
Risk Responsibility	Procurement Procedures Committee
Risk Mitigation Support	PSS, SAM Team

Recommendations:

We recommend that:

- a) Contracting templates be updated by the SAM team with input from PSS as to what is required in each form and made available in a manner that is easily accessible for staff. If this functionality is not available with the current system, a project should be initiated to find alternatives that will allow for better functionality.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Procedures Committee	a. ERPS and PSS will work together to address the issue of current forms being updated and uploaded in SAM.	Fall 2019

Observation 5

Duplicate names in SAM for both suppliers and bidders.

Multiple names of the same supplier and/or bidder creates inefficiency throughout contract management processes. Two prior attempts have been made by PSS and the SAM team to clean up supplier and vendor records, yet this continues to be an issue for the PSS team.

Risk Profile:

Risk Rating	High
Risk Impact	Inefficiency in contract awards, communication with suppliers/bidders and the potential for GNWT reputation risk.
Risk Responsibility	Comptroller General
Risk Mitigation Support	PSS, SAM Team, FESS

Recommendations:

We recommend that:

- a) The vendor list should completely and accurately reflect all current vendors. All duplicates should be identified and cleared from SAM.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. FESS will be undertaking a review to identify duplicate vendors and take appropriate action.	March 2020

Observation 6

Department feedback suggests that regional areas are not as well serviced by PSS.

Feedback received indicated that services provided by PSS are inconsistent where departments operate in multiple regions. These regional locations do not have an assigned contact at PSS which adds complexity to seeking continuity in support of contracting services. This is in contrast to departments with more localized operations that have an assigned PSS employee, as well as a back-up for any work absence. These assigned individuals build up a knowledge base through working with their assigned department which enhances the efficiency of contract services and ultimately value to the department.

Risk Profile:

Risk Rating	High
Risk Impact	Lack of assigned PSS staff results in poorer service levels and inefficient contracting processes.
Risk Responsibility	Director, PSS
Risk Mitigation Support	Departments

Recommendations:

We recommend that:

- a) PSS review the assignment of staff to departments with regional operations to seek continuity and consistency of services for greatest value to the department.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Shared Services	a. Regional contacts are identified and listed on the Procurement Share point site, accessible by all departments. When we have a staff shortage, the Manager, PSS emails the Superintendent and advises the names or team assigned to cover. The Director will complete a review and if applicable, will assign staff appropriately to seek continuity and consistency of services for greatest value to the department. PSS has also had some challenges in filling positions in the regions. As an example we have tried to hire a Senior Procurement Specialist in Fort Smith over a year without an success.	March 2020

B. TRAINING & AWARENESS

An assessment of training was completed as part of each departmental interview process. Modules created and posted for general staff access and training were inventoried and are set out below. Training is essential to ensuring staff are equipped with the knowledge necessary to meet the responsibilities within their roles.

Internal Control Capacity Model Rating

The control framework for Training & Awareness was rated as Ad Hoc. While training programs have been created and made available both online as well as directly from PSS, use of these tools are inconsistent at best. Compounding this is that training is not specifically identified and assigned for particular roles within the P2P cycle or for the varying levels of authority assigned throughout this same cycle. While training is available, a set framework for ensuring training is completed and for ensuring increasing levels of authority receive more training is lacking.

Observation 7

Training is not formalized by role or by level of authority.

As with all processes, an essential step is in ensuring staff are properly trained and appropriately equipped to perform their roles. As part of this work, a high-level review of training options was carried out.

Review of Training Options

P2P training modules were assessed for adequacy of training developed and made available for staff. Although each department is responsible for ensuring their respective staff have received adequate training, training tools on the following topics have also been made available centrally for all staff to access:

- Request for Proposals (RFPs): How to write, evaluate and award – introductory
- Request for Proposals (RFPs): How to write, evaluate and award – advanced
- How to manage your contract
- How to purchase goods and services under 25K with the revised sole source limits
- Working with procurement shared services
- eProcurement advanced training
- eProcurement training for boards and agencies
- eProcurement – SAM requisition training

- PeopleSoft 9.2 / SAM / Billing
- PeopleSoft 9.2 / SAM / Cash drawer entry
- PeopleSoft 9.2 / SAM / Delegated authority entry and maintenance
- PeopleSoft 9.2 / SAM / Expenses
- PeopleSoft 9.2 / SAM / External events
- PeopleSoft 9.2 / SAM / Inquiry
- PeopleSoft 9.2 / SAM / Journal entries
- PeopleSoft 9.2 / SAM / credit card cardholder
- PeopleSoft 9.2 / SAM / credit card coordinator

- PeopleSoft 9.2 / SAM / P2P / Accounts payable & vouchers for department representatives
- PeopleSoft 9.2 / SAM / P2P / Online expenditure approvals
- PeopleSoft 9.2 / SAM / P2P / Purchase orders
- PeopleSoft 9.2 / SAM / P2P / Requisition

- PeopleSoft 9.2 / SAM / FESS / Accounting clerks
- PeopleSoft 9.2 / SAM / FESS / Approvers

- PeopleSoft 9.2 / SAM / FESS / Supervisors

While the training modules above address many critical processes within the P2P cycle, interviews with the departments revealed there are no formally implemented training plans for specific roles (taking into consideration purchasing authorities as well as other duties relating to P2P) which are required in relation to the P2P cycle. Supplementing that which is offered above, PSS also offers courses directly to departments. Specific guidance is required for training requirements else the above training modules will not be accessed and used for their intended purpose. If not providing direction, departments will then fall back to conducting ad hoc training, person-to-person training, or training that is no longer applicable to new system upgrades and/or business process changes.

Risk Profile:

Risk Rating	High
Risk Impact	When training is left up to a department, rather than prescribed by role and/or authority level, employees may not be adequately trained for the duties they have been assigned as part of their role. It is also inefficient to have differing training methods when all P2P activities must go through PSS and FESS which are centralized.
Risk Responsibility	DM Shared Services Committee
Risk Mitigation Support	PSS, Departments, SAM

Recommendations:

We recommend that:

- Training programs be developed for staff identifying courses which must be taken in accordance with both role and authority level within the P2P cycle. In addition, training should be conducted consistently across all departments.
- Training completed should be monitored and tracked to ensure new employees receive training in a timely manner.
- Training completed should be monitored to ensure all employees receive training on new business processes and/or system upgrades.
- Access to certain aspects of SAM should be limited until specific training has taken place.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Procedures Committee	a. The OCG will review all current training within the P2P cycle and develop a plan to address gaps.	March 2020
	b. ERPS is looking to implement a learning management module in the human resource system which would address monitoring and tracking of training.	March 2020
	c. ERPS is looking to implement a learning management module in the human resource system which would address monitoring and tracking of training.	March 2020
	d. ERPS can only monitor this once a learning management module is available in the human resource system.	March 2020

C. PROCUREMENT

Results from audit procedures conducted are split between this section and Section C: Contract Management. Observations related to contract initiation, approval and final setup are discussed in this section. Observations related to the handling of contracts post setup are discussed in Section C.

Internal Control Capacity Model Rating

Procurement Guidelines, policies and procedures have been developed to ensure compliance with the FAA. Review of this documentation identified that some of the Procurement Guidelines provide contradictory guidance to that stated in the Service Partnership Agreement previously set up in May 2013. For example, there is differing guidance in relation to the responsibility for obtaining WSCC clearance in each document. When training is left up to a department rather than prescribed by role and/or authority level, employees may not receive adequate training for their respective duties. It is also inefficient to have differing training methods when all P2P activities must go through PSS and FESS which are centralized. This lack of consistency in guidance documents has contributed to the confusion in roles associated with the responsibilities of PSS and that of the departments. Although the guidance documents are in place and there is clarity around many of the procedures, the departments do not always follow these processes. In addition, it was found that departments are undertaking contracts with vendors which should be prepared with the assistance of PSS. The control framework has therefore been rated as Repeatable.

Compliance with “Values and Guiding Principles of Public Procurement”

Values and guiding principles of public procurement are identified by the National Institute of Governmental Purchasing (October 2010) as follows:

- Accountability;
- Ethics;
- Impartiality;
- Professionalism;
- Service; and
- Transparency.

GNWT policies, the Service Partnership Agreement, and the Procurement Guidelines were reviewed to assess their alignment with the above principles. Clear guidance was found which mirrored the above and was reflected in the following principle statements:

- Competition: complete the contract for the best value, on time, on budget, and meeting the program requirements;
- Transparency: ensure vendors have fair access to information regarding procurement opportunities, processes and results; and
- Socioeconomic Impact: Support the involvement of northern and local workers and businesses.

Procurement Guidelines also emphasized the need for government procurement activities to avoid inappropriate procurement practices and decisions and that pertinent legislation and contract law are to be complied with at all times. Specific roles have been assigned to PSS and the departments in the Service Partnership Agreement to ensure impartiality is supported throughout the procurement process.

Results of Substantive Testing

Substantive testing was conducted for departments selected for testing; INF, FIN & HSS (see Appendix E). Testing evaluated contracts created as well as the role played by both the department and PSS. Contracts were randomly selected for testing and were traced from PSS through to the departments. Request for Proposal / Request for Tender (RFP/RFT) files and sole source files were the focus of this testing as they were determined to be higher risk due to dollar value, complexity of contracting, as well as the likelihood of misuse for the underlying transaction.

Sample sizes were initially established to be comprised of 10 RFP/RFT and 10 sole source contracts. An assessment was conducted of the processes followed to ensure appropriate competitive bid through to final contract award. Actual files chosen were 58 in total as FIN had only 8 RFP/RFT contracts applicable in the period selected for testing. Results of testing completed are outlined as follows:

PSS Testing

PSS documentation for contracts was generally complete and maintained in the contract's respective files to support compliance with the Procurement Guidelines. A challenge noted during testing was that contract information/data can be stored in various locations which created confusion in locating specific documents for testing.

Observations from the contracts reviewed at PSS for the samples chosen from INF, FIN and HSS have been outlined in the following table:

Issue(s) Noted	Number of Occurrences
Consensus Proposal Evaluation form not signed	1
Sole Source was for an amount under the limit, but there were additional change orders which raised the total by over 30%	2
No emails / letters of regret on file	5
WSCC not on file	3
Nothing in the file documenting the review by PSS (sole source)	6
PO amount put through with large error, and not noted during review/finalization	1
Proposal from vendor not on file	4
Award letter not sent (posted on site and contract signed)	1
Insurance Certificate not obtained	1

Department Testing

Observations from contracts reviewed within each department for samples chosen from INF, FIN and HSS have been outlined in the following table:

Issue(s) Noted	Number of Occurrences
Performance evaluations not performed	8
Safety evaluations not performed (when applicable)	4
WSCC final clearance certificate not on file (when applicable)	7
Safety orientation minutes not on file (when applicable)	3
Insurance certificate not on file (when applicable)	10
WSCC letter of good standing not on file (when applicable)	6
SAM PO missing	9
SAM requisition missing	8
Safety orientation checklist not on file (when applicable)	3

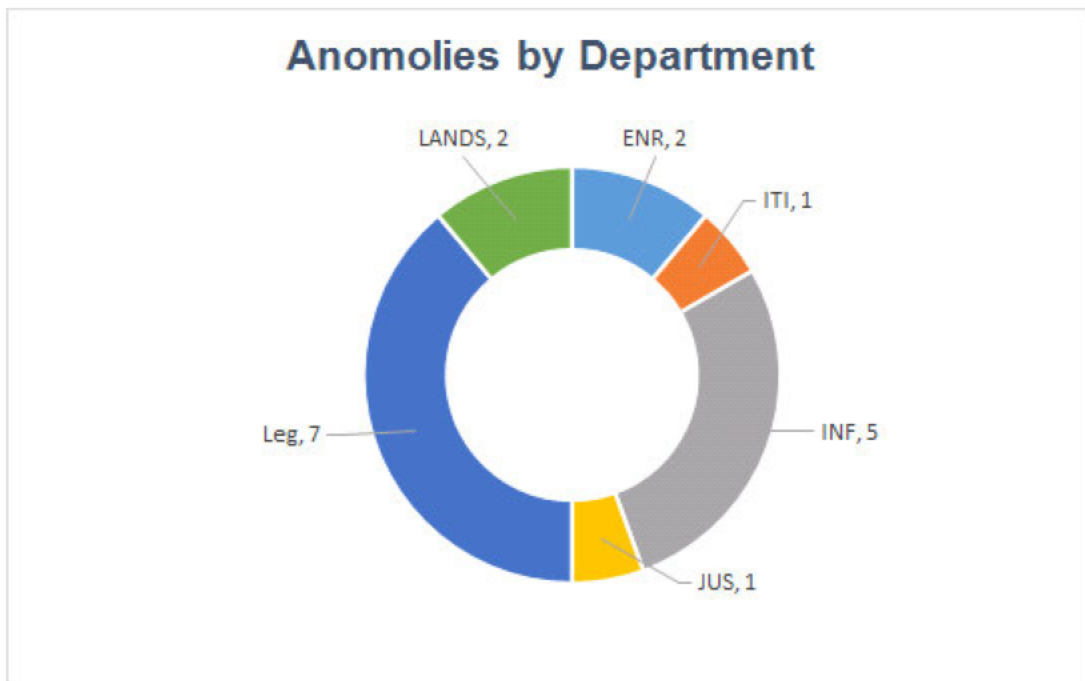
Observation 8

Contracts are created outside PSS guidelines and processes.

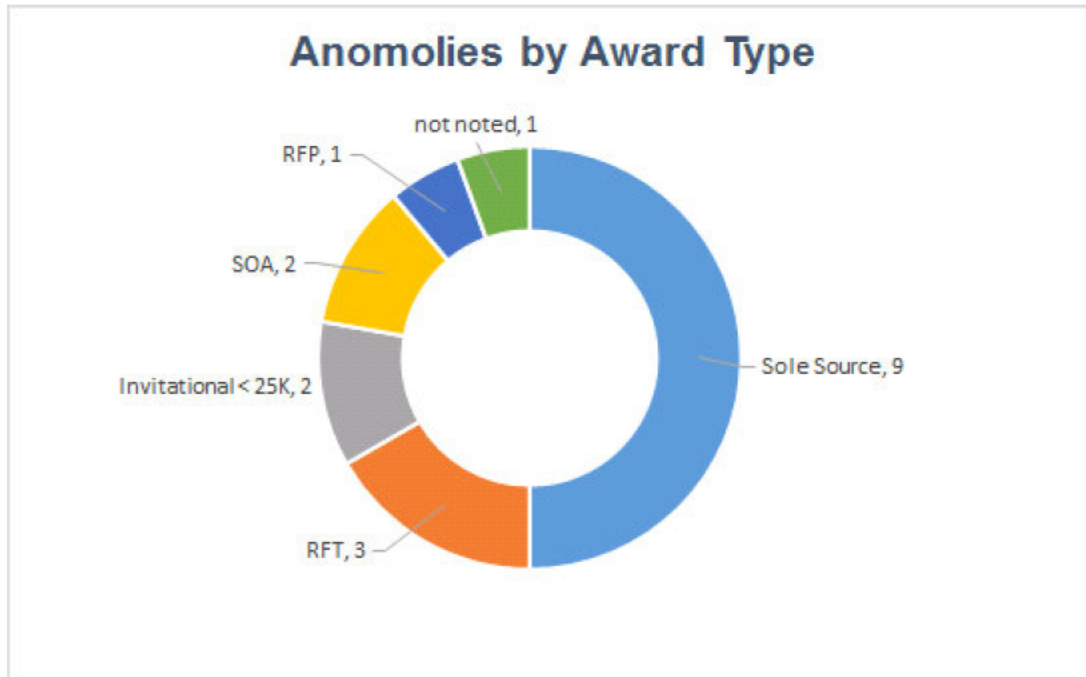
SAM versus PSS Contracts

Contract testing performed above was based on contracts processed through PSS. Details of contracts were obtained from SAM for the period April 1, 2018 to January 31, 2019. This data assisted in identifying the number of contracts processed by a department without the involvement of PSS. It is expected that some construction-related contracts are processed without PSS, as well as transactions related to the Fire Management Division’s SOA (due to timing issues in fire season), HSS’ medical/surgical equipment (they currently have an in-house process for this which will move over to PSS in April of 2019), goods under \$25,000, services under \$10,000, and architectural/engineering/professional services within set parameters. This leaves a category of “Other” representing contracts which should have been processed through PSS.

The composition of this “Other” category was 18 contracts worth a total of \$2,621,745. These contracts are being processed outside the requirements set forth in the Procurement Guidelines. During interviews with the individual departments, it was noted that some of these contracts related to scenarios where departments chose to move forward feeling it was in their authority and that they could support the decision to do so, whether to the Legislative Assembly or to the general public. A further breakdown of the 18 contracts into their respective departments are as follows:



These 18 contracts have also been depicted by type of contract prepared outside of PSS, as follows:



PSS has the expertise, and provides guidance to departments including tools and templates, to mitigate risk related to the acquisition of goods and/or services. By not using the services of PSS, variances to standard practice or contract terms and conditions can introduce risk to the GNWT. Departments may not have the appropriate knowledge and/or experience to effectively and efficiently enter into contract with vendors or service providers. This is why the Procurement Guidelines have been established to require PSS involvement.

An additional risk is that these contracts are not included in the reporting that PSS produces and that FMB relies on. If this data is not contained in this report, and does not appear to be reported elsewhere, then FMB is not seeing the full picture of the current status of contract files.

Risk Profile:

Risk Rating	High
Risk Impact	Increased risk of non-compliance with legislation, policies and/or procedures; terms and conditions of contractual obligations may open the GNWT to unwarranted liability(s). Reporting out to FMB may be incorrect or missing data as the contracts outside of PSS are not clearly reported elsewhere.
Risk Responsibility	DM Shared Services Committee
Risk Mitigation Support	PSS, Departments, FESS

Recommendations:

We recommend that:

- a) Departments should remind their staff of the services provided by PSS, and the Procurement Guidelines requiring use of PSS, to effectively contract for goods and/or services.
- b) A review of the PSS Service Partnership Agreement and Procurement Guidelines should be conducted to ensure that the assignment of roles and responsibilities between PSS and Departments is clear.

- c) Item (b) above identifies a greater need for a review of all roles and responsibilities between departments and each shared service; a full review of all guidance documents should be performed by both PSS and FESS.
- d) Routine monitoring by departments should be conducted to identify contracts completed without the use of PSS. Where contracts are identified as such, conduct a high level risk assessment to ensure the risk to the department, and GNWT, is appropriately mitigated.
- e) A SAM report showing all contracts should be compared by PSS to the PSS reports each month, and follow-up taken on contracts not processed through PSS. Follow up should take place to ensure these contracts are clearly reported to FMB. Initial review should be done of the 18 contracts noted in Appendix K.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Procedures Committee	a. PSS will ensure staff are aware of their services through business processes, information sheets and training that is already provided.	Ongoing
	b. PSS service agreements are in the process of being updated.	March 2020
	c. FESS reviewed and updated all business processes in January 2018 including departmental consultation.	Complete
	d. A process will be developed to identify completed contracts which should have been completed in the scope of PSS services.	March 2020
	e. Through (d) above a process will be developed to identify these contracts and appropriate action taken through partnership and training to ensure contracts that are in the scope of PSS services are completed through PSS.	March 2020

Observation 9

PSS observations on contract files are not consistently documented and placed on file.

Notes on PSS files denoting review by PSS staff, including their opinion, were noted as incomplete or missing on 12 of the 58 files tested. In some cases it was in relation to files where PSS did not agree with the contract decision made by the department on sole source contracts. While some supporting evidence of the agreement/disagreement could be found via email or other documentation, formal notation included in the contract file was not prepared and/or could not be found.

The role of PSS is to provide specific expertise to contracting decisions considered by departments. Having this expertise housed centrally removes the need for each department to hire personnel required to make these same assessments. This is necessary to appropriately mitigate risk to any of the values and guiding principles of public procurement.

Risk Profile:

Risk Rating	High
Risk Impact	Lack of PSS review documentation may result in breach of the values and guiding principles of public procurement; may also result in breach of policies and/or Procurement Guidelines.

Risk Responsibility	Procurement Procedures Committee
Risk Mitigation Support	PSS

Recommendations:

We recommend that:

- a) PSS ensures it reviews and provides related observations in regards to contracts (including sole source) which are maintained on file. This should include both positive (agreement with reasoning for decision and why) and negative (disagreement with reasoning for decision and why) observations.
- b) An annual report should be provided from the Director, PSS to the Procurement Procedures Committee outlining anomalies on files, including situations where PSS did not agree with the contract decision.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Shared Services	a. The procurement method (RFP, RFT RFQ, SOA Release, etc) should be the responsibility of PSS and not client departments excluding sole-source contracts. Client departments are responsible for justifying and defending their own sole source contracts. A reporting process will be reviewed.	March 2020
	b. PSS Director will investigate the option to prepare an annual report outlining anomalies on procurement files.	March 2020

D. CONTRACT MANAGEMENT

Contract management extends beyond initial approval and setup through work completed by both PSS along with the department. It is important to delineate this as the bulk of contract management responsibilities reside with the departments as opposed to PSS.

Internal Control Capacity Model Rating

The control framework in place relating to contract management has been rated as Ad Hoc. Consistency of contract management is varied by department. Incomplete contract files were routinely found across departments selected for testing. Contract file maintenance is not in accordance with records management guidelines as different locations were used to store documentation both electronically and in hard copy. The lack of clear delineation in regards to roles and responsibilities, what information is to be stored and by whom after the contract has been finalized with PSS, and a lack of a formalized vendor assessment process depict a weak control environment.

It was noted during fieldwork and interviews with departments that IT systems are not always trusted due to questions of accuracy of data, timing of transaction processing, and/or ability to directly access this information in SAM. This has driven some staff in the departments to use Microsoft Excel to track payments as they are not comfortable relying on SAM to provide the information required.

Also of note were that formal contract management responsibilities were not being completed by the individual departments. Documentation such as safety notes were missing from files, checklists for contract maintenance provided by PSS were not being used, and WSCC documentation was also missing. Critical documentation is necessary to ensure contract risk is sufficiently mitigated, vendor performance is assessed and monitored, and that liabilities to the GNWT are adequately managed.

Observation 10

Change order monitoring and tracking is not in place at PSS.

During the review of contracts, it was noted that there were two INF sole source contracts for which change orders accounted for more than 30% of the initially approved contract value. One began with a contract for \$53,980 and then had change orders for \$16,000 4 months later, and another for \$75,000 more than a year later. The second contract began at \$80,000 and then was increased by \$20,000 and then \$25,000 three months later. Sole source contracts are by nature a higher risk as compared with a competitive bid/formalized tender process. The lack of competition gives rise to many risks, two of which are: i) the value for the purchaser may not be optimized; and ii) increased risk of corruption in that the buyer and supplier may develop a relationship that is too close to the potential detriment of the purchasing entity. This risk is mitigated by the use of a lower dollar limit on most sole source arrangements, or the need for special approval to allow for that limit to be exceeded.

When change orders are used to increase the sole source value over time, it suggests that the contract may have been of larger value than originally presented for approval. Without a system to formally monitor and track change orders to ensure compliance with the 30% limit the risk of misuse increases.

Risk Profile:

Risk Rating	High
Risk Impact	Use of change orders to increase the value of a sole source contract by a significant amount may suggest that the initial value was understated and that the competitive bid/formalized tender process was purposely avoided. Lack of monitoring increases the risk of this occurring.
Risk Responsibility	Procurement Procedures Committee
Risk Mitigation Support	Director, PSS, Departments

Recommendations:

We recommend that:

- PSS, as part of its service offerings, be advised of all change orders, and maintain tracking of each. When change orders are large, or repetitive, a review should be performed to determine if misuse of sole sourcing has occurred.
- An annual report should be provided from the Director, PSS to the Procurement Procedures Committee outlining anomalies on files, including files where sole source change orders exceeded 30% of initial contract value.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Shared Services	a. PSS will look to offer this service as part of its service offering. PSS will work with ERPS on a reporting process.	March 2020
	b. PSS will work with ERPS on a reporting process if required.	March 2020

Observation 11

Contract file management is lacking.

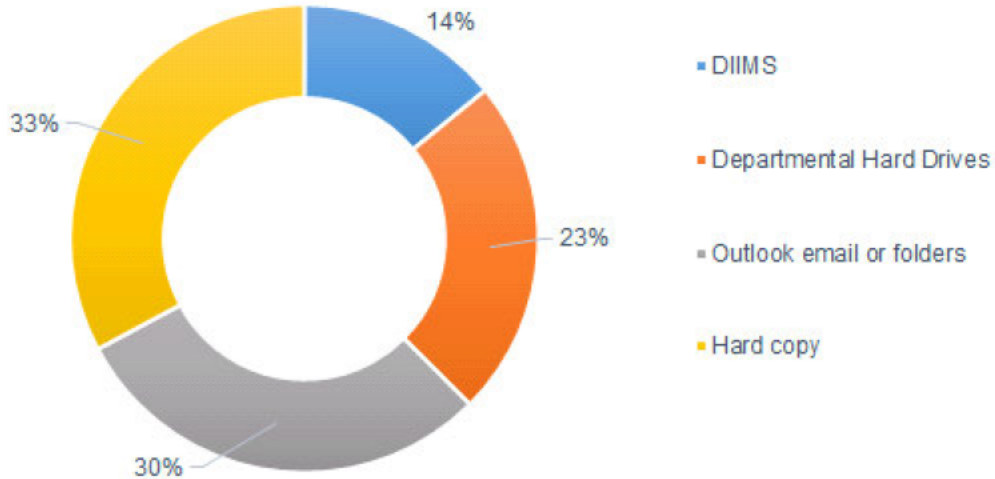
File storage methods in PSS and the departments are not consistent and/or not aligned with Records Management Guidelines.

During the review of both PSS and department contracts it was noted that filing in departments was not consistent. This can lead to confusion both within PSS as well as a department, and also between them if documents cannot be easily located as required. Procurement Guidelines define the retention

requirements for documents and that a Contract Management File be maintained. There is no delineation between hard copy and electronic version, yet the file should contain all relevant documents. Having documents randomly located throughout various mediums including Microsoft Outlook do not meet this requirement.

Documents were found to be stored by departments as follows:

File Storage Methods - Departments



Contract Management Checklist is not being used

Testing of contract files revealed that some did not include the respective requisition or PO for the related good and/or service. The approved requisition is noted in the Contract Management Checklist of the Procurement Guidelines as one of the items to be kept in the file as it has “been used during the contract process by PSS and are tools to be used by the client (department) to aid in managing the contract to completion”. The PO is valuable to the file to ensure proof of approval for the good and/or service. Crowe identified that PSS provides a Contract Management Checklist to each department as part of their involvement with the contract process. However, it is often not used by departments and the section related to PSS is not always completed before the file it passed to the department.

The Contract Management Checklist provides a list of documents that PSS places in the file, as well as a list of documents that would be required by the department. This helps ensure that all relevant items, such as approved requisitions, WSCC clearance, etc. is included in the file. Currently this checklist is only being used on a sporadic basis by departments.

Risk Profile:

Risk Rating	High
Risk Impact	Contract files are incomplete and lack the minimum information necessary to manage the vendor relationship, including ultimate payment for goods and/or services received. Tools which would assist in mitigating this risk such as the checklist are not being used.
Risk Responsibility	Procurement Procedures Committee
Risk Mitigation Support	PSS, Departments, Records Management Committee

Recommendations:

We recommend that:

- a) A department-specific protocol be developed to ensure a consistent approach to contract file management to ensure completeness of each file in accordance with the requirements set out in the Procurement Guidelines. This protocol should tie through to the Records Management Guidelines in place at GNWT.
- b) A periodic review should be carried out by each department to perform a quality assurance assessment on their contract files for completeness, accuracy and compliance with the Procurement Guidelines and Records Management Guidelines.
- c) Electronic contract files should also be maintained in accordance with the Records Management Guidelines.
- d) Testing on a periodic basis of a sample of each department's files should be re-implemented by PSS.
- e) PSS complete the checklist before it is sent to a department for each contract file, and provide related training on a set periodic basis for its use.
- f) Departments ensure that the checklist is understood and used by all contract management staff and is maintained with the contract file.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Procedures Committee	a. A review of current policies will be undertaken by the OCG.	March 2020
	b. A review of current policies will be undertaken by the OCG.	March 2020
	c. PSS is investigating a digitization program and a fundamental change to records management for PSS. Client departments are responsible for their own Contract Management files.	March 2021
	d. PSS will re-implement a process to sample departmental files	June 2020
	e. PSS has already implemented new procedures and auditing function to ensure all checklists are completed and all files updated appropriately for PSS contract file. The Contract Administrators review checks and files to ensure they are complete prior to filing them. The Contract Management checklist is a tool provided by PSS to departments to ensure they have the correct documents in their folders. The client department maintains the contract management file.	Complete
	f. PSS delivers contract management workshops.	Ongoing

Observation 12

Formal vendor assessments are not performed.

Interviews with each department, PSS, as well as results of substantive testing performed on contracts, formal vendor assessments are not being performed. During fieldwork only one specific instance was found where a vendor assessment was in the process of being completed. The department was ENR who had a very negative experience with a vendor and was working with PSS to complete an assessment and have it noted on file that this vendor did not perform in accordance with expected terms and conditions of their contract.

Formal vendor assessment processes are not in place either at the PSS or department levels. Reviews are valuable as they bring to light any issues that have occurred during work performed, or goods that were not of the quality expected. This will help to ensure sub-standard vendors are not used by other departments moving forward.

Risk Profile:

Risk Rating	High
Risk Impact	Lack of vendor review could result in sub-standard vendors being hired to provide goods and/or services in other departments impacting costs to the GNWT as well as bringing potential liability.
Risk Responsibility	Procurement Procedures Committee
Risk Mitigation Support	Departments, PSS, SAM Team

Recommendations:

We recommend that:

- A GNWT-wide policy should be developed to implement vendor reviews on a periodic basis with the results centrally stored for easy access by all departments for use in the competitive process.
- Departmental training and forms should be provided by PSS for this process.
- As part of contracting with vendors, a mandated step prior to signing contracts should be to review historic performance assessments. Additional consideration and explanation should be provided where a review was historically sub-standard and yet a department is again deciding to use the same vendor.

Management Response:

Area	Action Plan:	Completion Date:
Procurement Procedures Committee	a. Vendor assessment forms exist today. The PPC is reviewing an approach to track and monitor vendor performance for use as a management tool in assessing vendors. This includes looking at policy development.	March 31, 2021
	b. PSS will continue to promote and compile vendor assessments forms.	Ongoing
	c. The PPC is reviewing an approach to monitoring vendor performance to use as a management tool. This includes looking at policy development.	March 31, 2021

E. PAYMENT

Internal Control Capacity Model Rating

There are clear processes and procedures in place for FESS and the departments to effectively delineate roles and responsibilities. Automated approval authorities, documented procedures for FESS staff in processing payments, as well as real-time monitoring of payment processing activities within DIIMS create a strong control environment.

While there are set processes in place, they are not consistently followed. Although invoices are required to be sent directly to FESS for processing, often they are sent directly to the departments and forwarded to FESS, potentially resulting in payment delays. There are also circumstances where departments request that copies of invoices be sent to them; this also creates confusion and can result in duplicate payments. It was also found that payments are periodically processed by departments via AP voucher when they should have been paid directly through FESS. Lack of consistency in compliance with policies and procedures increases the risk that payments will not be timely, or that duplicate payments may be made. The control framework is therefore rated as Repeatable for this area.

Observation 13

Payment processing times are not in accordance with the FAM.

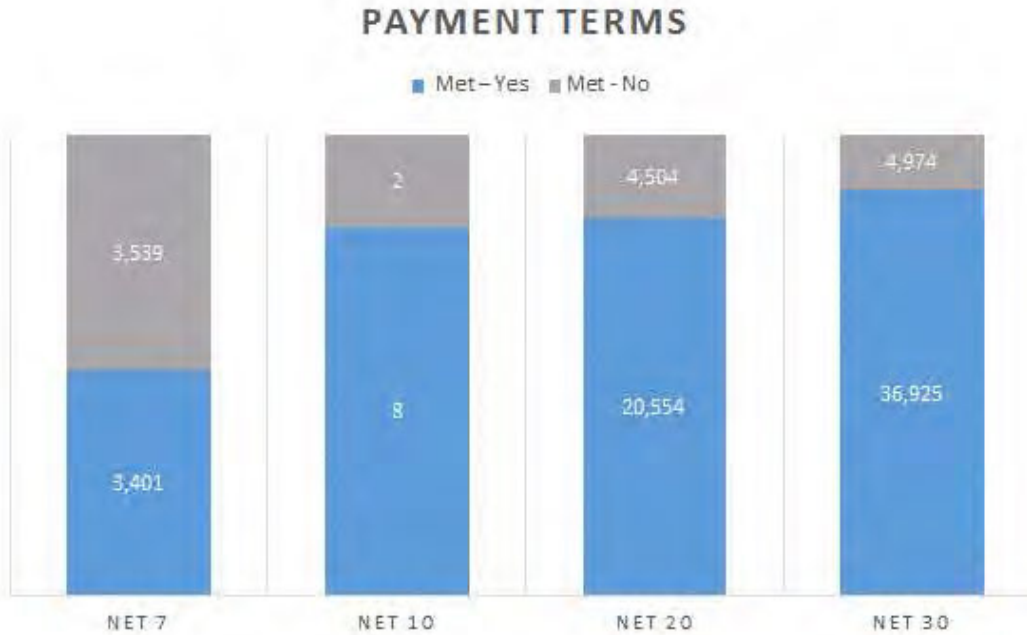
Within Section 700 of the FAM, sub-section 720 establishes timing for payment processing of individual transactions. Terms established are as follows:

Terms	Category of payment
Net 0	Public Officers and members of the Legislative Assembly
Net 7 and Net 10	Vendors that offer early payment discounts; when appropriate
Net 20	Vendors registered under the Business Incentive Policy (BIP)
Net 30	All other vendors

The SAM team provided data for voucher payments processed between April 1, 2018 and January 31, 2019. A comparison was then made of the “Entered Date” to the “Payment Date” based on the payment terms provided to determine how many vouchers were paid within the FAM parameters outlined above.

Through interview, FESS did note that metrics for payment processing are, at times, not reflective of actual payment processing activities but rather issues related to departmental responsibilities to submit invoices to FESS. When an invoice is submitted by a department to FESS, it is date stamped as at the date received by FESS, not the original date received by the department. A department may have held the invoice and not submitted it in a timely manner to FESS which would result in delayed payment and potentially late payment fees (i.e. interest). This was kept in mind during our testing and results of late payments by the GNWT. Also, payment of invoices can also be delayed due to the respective department confirming receipt of goods and/or services prior to payment being processed. FESS would need to wait on the department to confirm before payment can be made.

Based on the data analysis performed, the following results were noted:



Overall, the Government is paying 82.4% of vendors within the payment terms defined by the FAM. Within these statistics are the circumstances referred to above – whether the department submitted the invoice and/or validated the receipt of goods and/or services in timely manner. With respect to the findings within this report related to the treatment and inefficiencies of vendor invoices received by FESS, the department or both, additional attention is required to address the receipt and processing of invoices.

It should be noted that although the government is paying 88% of the regular vendors in a timely manner, payment terms for BIP vendors are being met only 82% of the time. The net 20 terms are established to provide incentives for BIP vendors and build relationships with local business. If these payments are not being made in a timely manner, that incentive is reduced and those relationships are not likely to be as strong.

Invoices processed outside of payment terms established by the FAM are caused by inefficiencies (FESS or department), PO match exceptions, default coding, timing related to resolving coding issues, as well as slow approvals by departments.

FESS performed a review of late payments in October 2018 and noted the same issues already identified. Remediation activities were recommended for both FESS (review of current business processes and identification of areas for improvement) and the departments (regular departmental reporting on vouchers in match exception status; a representative from payment-heavy departments such as INF work with FESS to develop more vendor templates to reduce default coded invoices; departments improve the process to ensure expenditure authority is consistently delegated when another authority is out-of-office). Crowe agrees with, and will continue to emphasize these recommendations, for all departments as outlined below.

FESS processes payment in accordance with the FAM guidelines through establishing automated payment release dates based on invoice receipt date. For example, a BIP vendor will be automatically paid 20 days after the invoice receipt date at FESS. However, should a department delay in submitting the invoice to FESS, any extent of delay will extend the actual final payment to the vendor.

Risk Profile:

Risk Rating	High
Risk Impact	Delay in vendor payments impacts the reputation of the GNWT; non-compliance with the FAM. Local business development incentives are lacking
Risk Responsibility	Comptroller General
Risk Mitigation Support	FESS

Recommendations:

We recommend that:

- a) Consideration by the Comptroller General be made as to whether the recommended remediation activities by FESS, based on their October 2018 review, continue to be relevant. If so, these processes should be implemented. The activities suggested are as follows:
 - Review current business processes and identify any improvement(s) required (responsibility of FESS).
 - Develop standard communications for FESS and the department contract managers (INF was used in the report but this would apply to all departments) consistent with the business processes.
 - Regular departmental reporting on vouchers in match exception status and purchase orders with exhausted balances to ensure issues are identified proactively.
 - A representative from each department to work with FESS to develop more vendor templates to reduce default coded invoices.
 - Departments to improve processes to ensure expenditure authority is consistently delegated when another authority is out-of-office.
 - A representative from the department work with Accounting Services to identify GNWT credit cards where the transactions limit is less than \$10,000 and raise the individual transaction limit. Departmental credit card controls should be reviewed regarding the credit card process.
- b) If it is determined that these activities would not adequately address the risk, an alternate plan for ensuring that the FAM conditions are met should be developed.

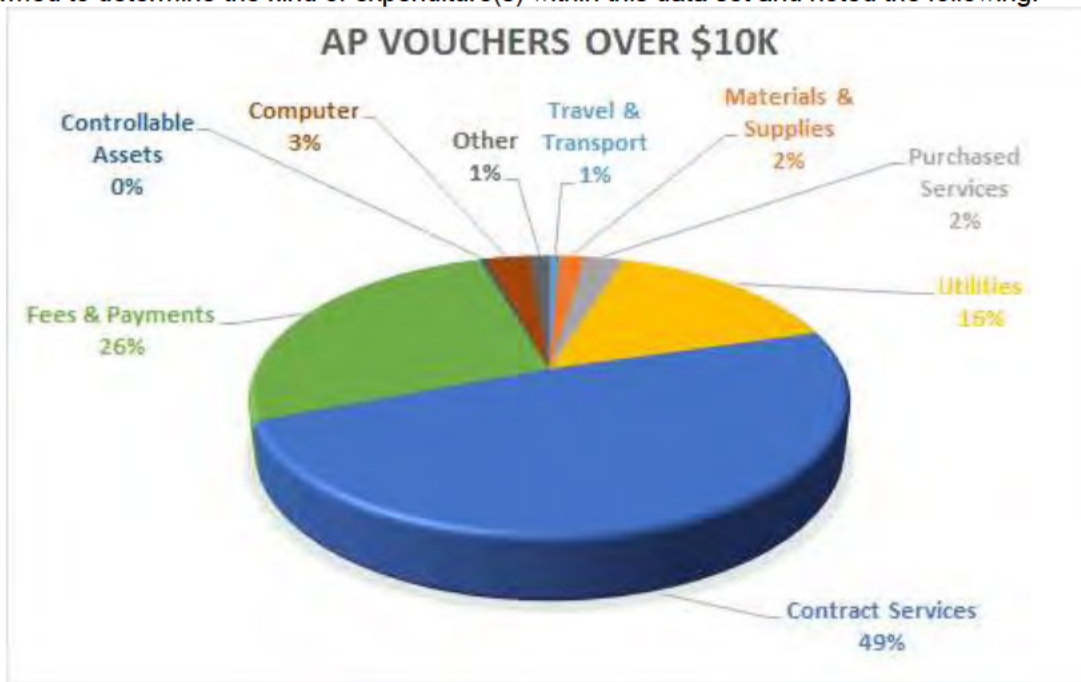
Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. Business processes were reviewed in entirety during the fall of 2018. Business processes include best practices for contract managers. Ongoing continuous improvement is in place. FESS will bring to the Finance Managers group information on how they can report on vouchers in match exception status and purchase orders with exhausted balances. FESS will be updating vendor templates and will be doing a vendor communication plan to ensure invoices are sent to the appropriate location.	Fall 2019
	b. Practices occurring in (a) will adequately meet the FAM provisions.	

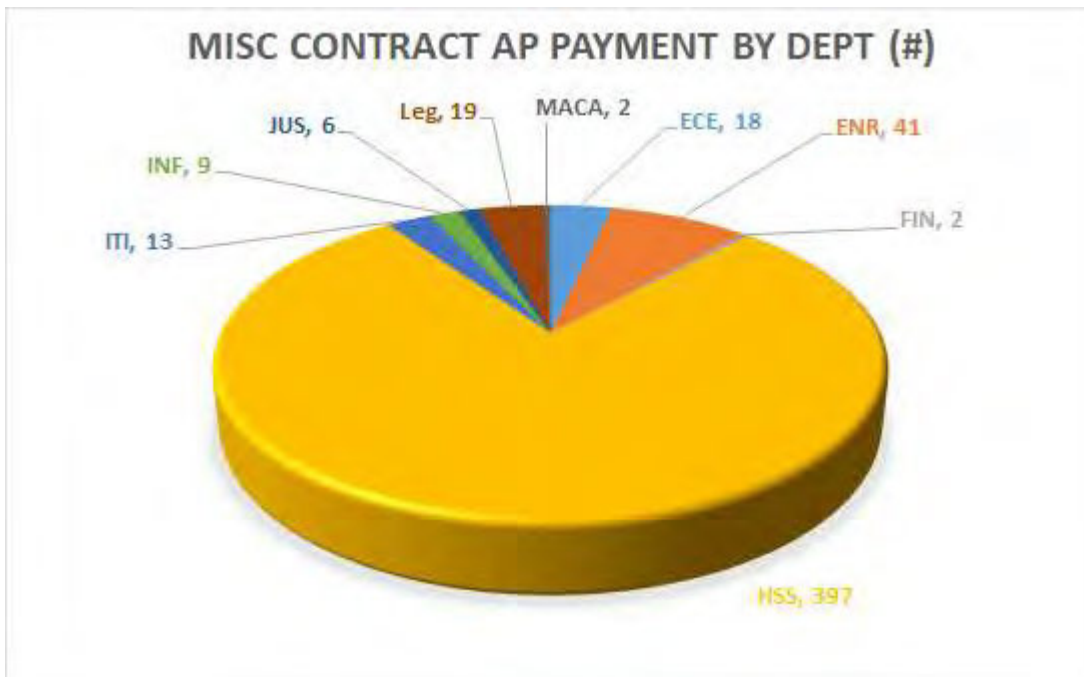
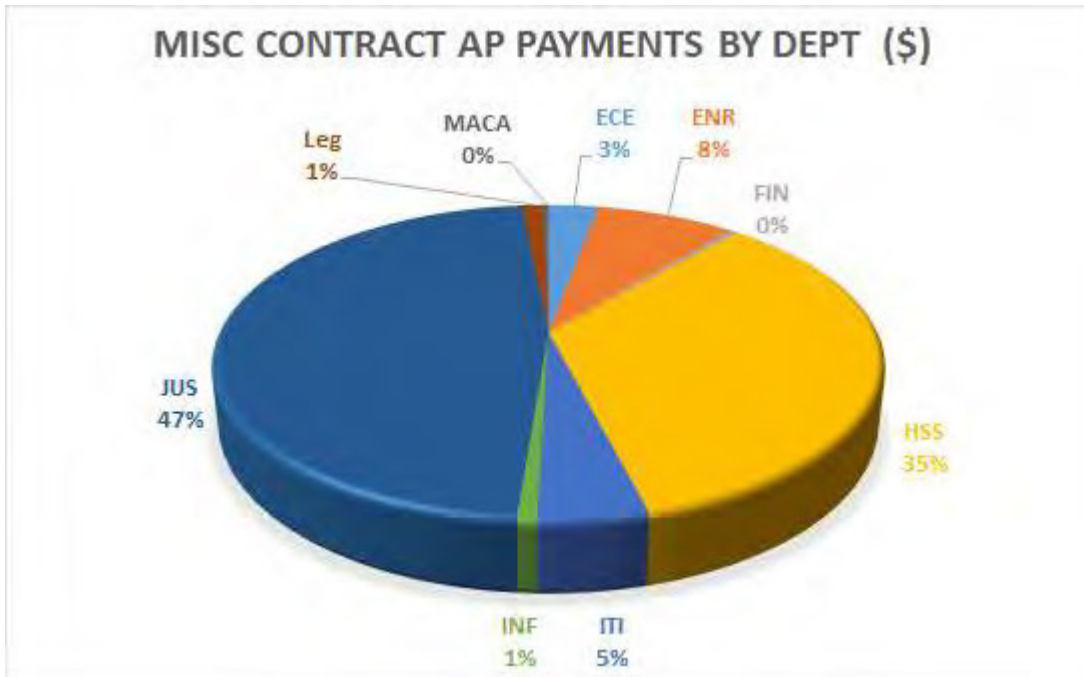
Observation 14

Payments are processed as AP Vouchers in the departments for items greater than the \$10K limit.

Data was obtained for the period April 1, 2018 to January 31, 2019 to evaluate the methods by which payments exceeding the GNWT credit card limit of \$10,000 may be alternatively transacted directly by a department. The data set was adjusted to remove standard transactions which relate to an approved SAM contract. 393 unique vendors were identified representing 2,399 payments over \$10,000. Chargebacks and interest were removed which resulted in 2,366 specific payments. An assessment was performed to determine the kind of expenditure(s) within this data set and noted the following:



Total payments were \$190,842,469. Of “Contract Services” which represents 49% (\$88,892,192) of AP voucher payments greater than \$10,000, 43% (507 payments totaling \$23,849,789) were categorized as “Miscellaneous Contracts”. These payments represent a greater risk as processing is undertaken directly by the department(s) versus FESS as defined within the Financial Shared Services - Service Partnership Agreement. Further review was performed to determine both number of contracts and dollar value by department for the payments noted as being for Miscellaneous Contracts. See below for findings:



If the two sets of data are combined, it shows that HSS has the highest level of AP payments when both number and dollar amount are combined. ENR, ITI and ECE have higher levels of these payments which should be reviewed. The high dollar value for JUS comes from one very large payment which should also be reviewed. Although the Leg payment dollars are small, the question arises as to why that number of payments was made via AP voucher and not through FESS.

Processing of these payments was moved from the departments to a shared services model within FESS to ensure consistency and efficiency for these types of transactions and to remove duplication of efforts

within the departments. The purpose of the shared service model is undermined when departments continue to undertake payments which are not within their defined responsibilities. Treatment of invoices has already been addressed earlier within this report. Additional work should be undertaken to identify the reason for the “Miscellaneous Contracts” discussed above and to clarify roles and responsibilities between FESS and the departments.

Payments are being processed directly by departments for goods and services greater than the \$10,000 when these are to be processed by FESS.

Risk Profile:

Risk Rating	High
Risk Impact	AP Vouchers may be processed for goods and/or services inconsistent with the policies and procedures established by FESS; departments undertaking work assigned to FESS creates confusion and inefficiencies including lack of consistency in payment processing.
Risk Responsibility	DM Shared Services Committee
Risk Mitigation Support	Departments, FESS

Recommendations:

We recommend that:

- Additional training should be implemented to ensure departmental staff working within the P2P cycle are informed of the need to use FESS for payments processed greater than \$10,000.
- Reporting of AP Voucher payments over \$10,000 should be reviewed by departments on a monthly basis to monitor for incorrect processing and to correct staff behaviors in a timely manner.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. Departments have business reasons for processing payments over \$10,000 with a VISA card. The ability to raise a VISA card limit to incur expenses of this value is controlled centrally. Departments are reminded that paying by VISA does not relieve them of the need to use proper procurement methods when they seek an increase. A document will be created to guide Departments in making sure that proper vigor is exercised.	Fall 2019
	b. A report will be made available to Departments to review payments over \$10,000 on VISA cards that can be run monthly by Departments.	Fall 2019

Observation 15

Invoice approval control may be missing.

Authority Limits Review

A high-level review of expenditure authorities was performed during this audit. The purpose was to analyze the different positions held by those with expenditure authority within the departments we selected for substantive testing as well as any consistencies/variances between each department. It is

important to monitor the risk that those approving expenditures have direct awareness of whether the goods and/or services have been delivered prior to processing payment.

Assignment of authority did vary by department in relation to the number of individuals assigned authority as well as the level of authority provided to each. While this may be expected to some extent due to the difference in department purpose and related activities, it does raise the question of authority assignment and the ability to link approval authority to those with direct knowledge of goods and/or services received.

INF:

Role	25K	50K	100k	250K	500k	1M	Total
Senior Manager						22	22
Manager	2	4	33	32	19		90
Senior Analyst			2	1			3
Specialist	1		2				3
Senior Officer	1		14				15
Officer	1	10	24				35
Analyst		3	1				4
Supervisor	2	8					10
Clerk	4						4
Total	11	25	76	33	19	22	186

FIN:

Role	25K	50K	100k	250K	500k	1M	Total
Senior Manager						20	20
Manager	1		2	29		4	36
Senior Analyst	4						4
Specialist	17					4	21
Senior Officer	11						11
Officer	40					4	44
Analyst	18					1	19
Supervisor			1				1
Assistant	9						9
Advisory	1						1
Total	101	0	3	29	0	33	166

HSS:

Role	25K	50K	100k	250K	500k	1M	Total
Senior Manager						17	17
Manager			21	1			22
Total	0	0	21	1	0	17	39

Where departments set expenditure authorities primarily with senior positions, it is paramount that a process be established to validate the delivery and quality of goods and/or services prior to payments being processed. This information is required to pay for goods and services received which meet the agreed contractual obligations by the vendor before payment is approved. Without this information, payments may be approved for sub-standard or non-existent goods and/or services.

Potential of missing control due to automation of approvals

Prior to the introduction of electronic purchase approvals, invoices were received by each department for coding and approval by staff as denoted above. Their approval on the invoice indicated to the payment authority that the goods and/or services were received and that they met contractual obligations as well as quality requirements. This was a key control to ensure payments were made only for goods and/or services actually received.

With the new automated process, all invoices are to be sent directly to FESS for processing and ultimate payment. The onus is now on the expenditure authority to contact their departmental staff responsible for the procurement transaction to ensure the goods and/or services were received prior to authorizing payment. This control is not formalized in policies, procedures or manuals and may be missed due to volume of expenditures processed monthly.

Risk Profile:

Risk Rating	High
Risk Impact	Payment may be processed to vendors for which goods and/or services have not been provided or do not meet contractual obligations.
Risk Responsibility	Comptroller General
Risk Mitigation Support	Departments, FESS, SAM Team

Recommendations:

We recommend that:

- a) Departments review their levels of purchasing authority and ensure approval for payment is only provided once confirmation of receipt of goods and/or services is received.
- b) This should be a documented process that all expenditure authorities be made aware of and receive training for their respective roles, including the risks related to their responsibilities.

Management Response:

Area	Action Plan:	Completion Date:
Comptroller General	a. The OCG will ensure guidance is provided to Departments to review expenditure authority, in particular when employees are moving departments for a new job.	March 2020
	b. Financial approvals training is available to all staff and will continue to be improved. Once an enterprise learning management system is in place this can be tracked appropriately.	Ongoing

APPENDIX A: ADDITIONAL BACKGROUND DETAILS

The following is meant to establish a high level overview and understanding of the 11 departments, PSS and FESS and how they interact within the P2P cycle. Assigned roles have been outlined in approved Service Partnership Agreements and are summarized as follows:

Procurement Shared Services (PSS)

PSS, within the Department of Infrastructure, acts as the main procurement hub for all GNWT departments, administering and managing larger GNWT procurement activities which are defined as:

- Procurement of all goods and services valued over \$25,000 for goods, and \$10,000 for services (excluding construction), from start to finish;
- Releases against Standing Offer Agreements (SOAs) over \$25,000;
- Procurement of air charters;
- Centralized Tender Desk for HQ and regional centers; and
- Providing contract advice and support to departments, boards, and agencies.

Financial and Employee Shared Services (FESS)

FESS, within the Department of Finance, provides financial transaction processing on behalf of GNWT departments and the NWTHC, as well as a range of employee services, such as payroll, data management, and benefits. FESS is responsible for:

- Providing services for suppliers including supplier set ups, supplier updates, direct deposit set-ups, and accounts payable;
- Approving, processing, and issuing payments for all invoices from vendors for good or services to all GNWT departments and NWTHC;
- Processing of transactions for goods under \$25,000 and services under \$10,000, only when:
 - The vendor does not accept the GNWT credit card;
 - There is a purchase order for the purchase;
 - The purchase is listed on the list of non-acceptable corporate purchase card purchases as per P2P-323 Purchase of Goods and Services Under \$10,000; or
 - The purchase is a utility payment and has a corresponding template.
- Providing services for customers which includes customer set ups, customer updates, on location cashier and accounts receivable; and
- Providing payroll and benefit administration services for the GNWT employee groups [outside of scope for this project].

Departments

Departments are responsible to identify the need for goods and/or services, which procurement procedures are to be followed (based on type and value of these goods and/or services), including when to involve PSS for guidance and assistance. Departments begin the requisition process which is then carried forward to PSS for processing. Departments work with PSS to establish the necessary procurement mechanism (i.e. Sole Source, SOA, SAA and RFP processes) as well as to structure and formalize a final contract. Departments make use of GNWT credit cards where the amount is less than \$10,000.

Legislation and Guidance

The FAA, FAM and Government Contract Regulations (GCR) direct how the GNWT should carry out procurement and payment activities within the P2P cycle. All policies, procedures, processes and systems should ensure compliance with the FAM and ultimately the FAA. Additional guidance can be found in the Procurement Guidelines, the Service Partnership Agreement between PSS and the departments including NWTHC, and the Service Partnership Agreement between FESS and the departments. Please note that a draft document has been created which is proposed to replace the Service Partnership Agreement between FESS and the departments. As at the date of this report, that document had yet to be ratified for implementation.

Supporting Systems

The PeopleSoft System for Accountability and Management (SAM) is used throughout the P2P cycle. Purchasing authorities are assigned within SAM, and approvals are performed electronically for most purchases. Exceptions exist for transactions related to GNWT credit card payments. These are paid directly with reconciliations required within SAM to validate and authorize all individual expenditures. Concerns were raised during the audit regarding inefficiencies of the current processes within SAM for procurement and have been addressed later in this report.

APPENDIX B: FAM ROLES & RESPONSIBILITIES

This table outlines the roles and responsibilities defined within the FAM in relation to significant P2P processes. Specific roles and responsibilities are assigned to different departments/shared services to ensure adequacy of oversight as well as to establish accountability for each step of procurement activity through to final payment approval and processing.

	Departments (All)	Finance	FMB	Common Service Groups	Comptroller General
Procurement	Deputy Head responsible to manage contracts to ensure procurement activities are in accordance with the procurement procedures established by the GNWT.	Deputy Minister Finance responsible to establish a standard Vendor Compliant Process for the GNWT to address complaints systematically in a rational, fair, reasonable, timely and consistent manner. Also responsible to establish a Procurement Procedures Committee to oversee the development of GNWT procurement procedures	FMB may issue a directive respecting the financial management or financial administration of a Public Agency.		May approve Interpretation Bulletins associated with this policy.
Contract Registry & Reporting	Deputy Head shall ensure that the contract data recorded is reviewed and updated regularly to facilitate timely and accurate reporting.		FMB may issue a directive respecting the financial management or financial administration of a Public Agency.		Ensures the public posting of a quarterly report for listing contracts for services over \$10,000 and contract for goods over \$25,000 that have been entered into during the period. May approve Interpretation Bulletins associated with this policy.
Commitment Accounting	Deputy Head responsible to ensure that regular analysis is undertaken to ensure that all known or estimable expenses will be accommodated within an approved appropriation or budget.		FMB to act on all matters related to the financial management and financial administration of Government in response of		May approve Interpretation Bulletins associated with this policy.

	Departments (All)	Finance	FMB	Common Service Groups	Comptroller General
			<p>expenditures plans, financial commitments and programs.</p> <p>May issue a directive respecting the financial management or financial administration of a Public Agency.</p>		
Timing of Payments	Deputy Head responsible to require sufficient internal controls to ensure that payments are processing within the timelines established in this policy.		FMB may issue a directive respecting the financial management or financial administration of a Public Agency.		May approve Interpretation Bulletins associated with this policy.
Corporate Credit Cards	Deputy Head responsible for ensuring that corporate credit card holders have adequate training and the required authorities in place prior to corporate credit card being issued; ensure internal controls to identify and prevent fraudulent activity and to ensure timely reconciliation of transactions by cardholders.				May approve Interpretation Bulletins associated with this policy.
Common Service Groups	Deputy Head responsible to ensure that designated common service groups operate to the extent by which they are mandated and that client agreements are approved and committed.		<p>May designate certain common service groups that will be funded on a full cost recovery basis.</p> <p>May issue a directive respecting the financial management or financial administration of a Public Agency.</p>	Responsible for providing substantiation and the application of appropriate terms, conditions, formulae, accounting and criteria for the agreement provided to the	May approve Interpretation Bulletins associated with this policy.

	Departments (All)	Finance	FMB	Common Service Groups	Comptroller General
				client Department or Public Agency.	
Disbursements	Deputy Head responsible to ensure that recording, verifications and approval of expenses is in accordance with an appropriation or applicable agreements.		FMB may issue a directive respecting the financial management or financial administration of a Public Agency.		May approve Interpretation Bulletins associated with this policy.

APPENDIX C: SERVICE PARTNERSHIP AGREEMENTS

This Table outlines the roles and responsibilities defined by the Service Partnership Agreements as applicable to the transaction level within the P2P cycle. While steps are being taken to update these roles and responsibilities regarding FESS, they were not considered for this audit as they were not fully adopted and implemented by management.

	Department	PSS (procurement activities)	FESS (payment activities)	SAM
Accurate & Timely Identification of the need for goods/services	Responsible	Assist as needed		
Determine appropriate method of procurement	Work with PSS	Work with Department		
Start Requisition in System	Data Entry		Approval	
Contract Advice & Support		X		
Responsible for procurement under \$25,000 for services and \$10,000 for goods	X			
Responsible for procurement for services greater than \$25,000 and goods greater than \$10,000 and determine the method of procurement		X		
Develop procurement plan	Work with PSS	Work with Department		
Manage competitive process		X		
Releases against Standing Offer & Service Supply Agreements	Work with PSS	X		
Evaluation Process	Assist as Needed	Responsible		
Expenditure Officer – approve expenses	X			
Receive, prep and validate vendor invoices & forward to expenditure officer			X	
Enter/upload details into AP module			X	
Validate Supplier details			X	
Maintain SAM vendor file	Request		Request	X
Maintain Vendor Payment file			X	
Reconcile vendor statements			X	
Check cost allocations, matching, authorization			X	
Process payment and distribute remittance advice			X	
Primary supplier/customer contract/resolve routine			X	
Credit cards	Cardholder verification & spending		Statement distribution & processing	
Travel Authorizations	Self-service / expenditures		Payment	
Expense Claims	Self-service / expenditures		Payment and prepay audit	

APPENDIX D: ESSENTIAL CONCEPTS (FAA AND GCR)

Outlined below are pertinent concepts and requirements of the FAA and GCR which have guided audit procedures undertaken during our fieldwork.

Financial Administration Act – Essential Concepts / Requirements

A person shall not incur an expenditure unless he or she is an expenditure officer.
Expenditures must be made only in relation to an appropriation as supported by the Estimates, and that there are enough uncommitted funds to commit to the expenditure. Expenditures must be consistent with the purpose of the activity set out in the Estimate on which the appropriation is based.
Disbursement must only be made on behalf of the government once it has been confirmed by an expenditure officer that there is money available for the purpose for which the disbursement is intended, and that the disbursement is consistent with the contract or agreement which outlines the purpose of the amount.
A person shall not enter into a contract or assume an obligation for or on behalf of Government that requires an expenditure unless the expenditure is being incurred pursuant to an appropriation, that all reasonable measures have been taken to ensure there are sufficient uncommitted amounts for this activity, and the expenditure is within the purpose of the activity as set out in the Estimates.

Government Contract Regulations – Essential Concepts / Requirements

A contract authority shall issue a tender before entering into a contract unless the contract authority believes, on reasonable grounds, that <ol style="list-style-type: none"> a) Performance of the contract is urgently required and delay would be injurious to the public interest; b) Only one party is available and capable of performing the contract; or c) The value of the contract will be less than: <ol style="list-style-type: none"> i. \$100,000 in the case of a contract for architectural or engineering services, ii. \$50,000 in the case of a contract for professional services other than architectural or engineering services, or iii. \$25,000 in the case of any other type of contract.
A request for proposals must state the criteria to be used in evaluating the proposals.
In evaluating a proposal, no criteria may be used other than those provided by these regulations or stated in the request for proposals.
Every tender and every request for proposals must be issued in writing and must specify <ol style="list-style-type: none"> a) The address to which the bids or proposals must be submitted; and b) The date and hour after which no further bids or proposals shall be accepted.
A contract authority shall, <ol style="list-style-type: none"> a) In the case of a tender, only award the contract to a responsible bidder whose bid is <ol style="list-style-type: none"> i. Responsive, and ii. Lower than any other responsive bid submitted by any other responsible bidder; and b) In the case of a request for proposals, only award the contracts to a responsible proponent whose proposal <ol style="list-style-type: none"> i. Is responsive, and ii. Will, in the opinion of the contract authority, provide the best value to the Government.

APPENDIX E: DEPARTMENTAL CONTRACTING RISK ASSESSMENT

All 11 departments were reviewed as part of this operational audit. These reviews specifically looked at the controls in place at each department and considered supporting documentation in areas determined to be of specific interest and/or risk significance. All departments were audited using interviews with management at each as well as a high-level review of policies, procedures and related control frameworks designed and implemented as at the date of the audit. A risk assessment (Appendix G outlines the risk criteria) was then performed on the departments to determine which would warrant specific focus and detailed substantive testing. The result of our initial risk assessment is contained in the following table:

Entity	Number Contracts	Value	Sole Source	Multi-year	Control Environ.	Value of Credit Card	# of Change Orders	Non-PSS Contracts	Audit (Y/N)
ECE									N
ENR									N ¹
EIA									N
FIN									Y ²
HSS									Y ³
ITI									N
INF									Y ⁴
JUS									N
Lands									N
Leg									N
MACA									N
Very Low		Low		Moderate		High		Very High	

Note 1: ENR was noted as being of moderate to high risk in areas such as GNWT credit card transactions, change orders, and non-PSS contracts. Although this was considered in regards to sample testing, these numbers were expected and not noted as exceptionally risky due to the nature of the department's procurement activities. Wildfire/forest fire suppression drives immediacy for response thereby bypassing PSS for contracts as the fire season begins. Routine processes and their related controls may delay critical expenditures required to fight these fires. GNWT credit cards are used regularly during this time to process immediate payment for goods and services required. The overall control environment was noted to be at moderate risk due to what appeared to be a disconnect between those managing the contracts at a higher level of management compared to those within the department. Additional follow-up was conducted with ENR personnel responsible for fire operations revealing a strong understanding of necessary controls and required processes for procurement through to payment activities. This area was therefore not chosen for specific sample testing.

Note 2: FIN was not rated as a higher area of risk, but was chosen for further sample testing due to the complexity of the department and the numerous areas to which it has oversight responsibilities. An additional factor considered was the overall value of contracts within the department which resulted in this department being selected for substantive testing.

Note 3: HSS was rated as a moderate risk in many areas including the number of sole source contracts. Sole source contracts bring an increased level of risk due to the nature of these contracts and that they are not subject to the competitive bid process. In addition, there were a larger number of change orders processed in addition to non-PSS contracts signed. This department was therefore selected for further testing.

Note 4: INF was rated as a high risk in many areas. There is a large volume of contracts processed through this department. This volume and the complexity of multi-year contracts has identified this department for further testing.

An assessment was also undertaken of the types of procurement activity which have the highest risk to each department. These were identified as those denoted as RFP/RFT in addition to those labelled as Sole Source. A sample of RFP/RFT and Sole Source contracts were therefore chosen for each selected department (see above) for additional testing. Results of testing are outlined later in this report. Although Multi-Year contracts are also of high risk due to the need for departments to manage ongoing changes and obtain updated WSCC Clearance and Insurance certificates/documents, it was determined during the interview process with departments that the controls in this area were not strong enough to warrant substantive testing. It was clear that the updating of certificates and other documents was not being performed by the departments as there was confusion regarding who was responsible between the department and PSS. Where Crowe finds either the design or the operational effectiveness of a control to have failed, no additional testing is then undertaken.

Not included in this work was testing related to the complaint process. It was brought to our attention during the planning process that a separate review was being performed in this area, therefore it was only confirmed that a process existed and no further review was performed.

APPENDIX F: DEPARTMENT RISK CRITERIA

Testing Criteria

Area of Testing	Ratings Method
Contracts (Total, Non PSS, Sole Source, SOA, Tenders)	Rated for each department as a percentage of the total number of that type of contract
GNWT credit card Transactions	Rated by the value of the GNWT credit card transactions for a department as a percentage of the total for all GNWT credit card transactions
Change Orders	Rated by percentage of the number of change orders for a department over the total change orders for all departments
Control Environment	Based on an assessment performed by audit staff of control environment rating based on initial interviews with management

Percent Ratings Categories

Rating	Percent Range
Very High	50-100%
High	25-50%
Moderate	10-25%
Low	5-10%
Very Low	0-5%

Description of quantitative and qualitative considerations to risk assess each department as applicable to P2P (qualitative assessments are subjective based on information received).

		QUALITATIVE					
Level	Impact	Number of Contracts	Value of Procurement	Sole Source	Multi-Year Contracts	Change Orders	Control Environment
5	Very High	18(a)					
4	High						
3	Moderate						
2	Low						
1	Very Low						

APPENDIX G: PSS & FESS APPROACH

Testing for PSS was approached in a similar manner to that of the departments. Interviews were undertaken with staff who have responsibility for procurement activities within the P2P cycle, including working with the individual departments. This included a review of current policies and procedures developed to provide the control environment necessary to guide contracting through to advice provided to the departments. Sample testing was performed consistent with the methodology established for the departments. The departmental risk assessment was used to select individual files which were then tested in both PSS as well as the department for their respective roles and responsibilities within the P2P cycle.

FESS processes relate to payment and vendor management activities within the P2P cycle. Interviews with management in FESS were also undertaken along with assessing their control environment. As all transaction processing has been digitalized, use of data analytics was relied upon to conduct detailed testing vs. placing reliance on sample testing and individual transaction substantive testing.

A list of data analytics carried out as well as data specifically requested from SAM to evaluate the P2P cycle at PSS, FESS and the departments is as follows:

Testing	Risk
Default Coding (at a point in time)	Invoices are not being allocated to a correct department and/or not being processed in a timely manner
PO Match Exception Report	PO does not match correctly to invoice
Comparative of DIIMS workflow – emails for invoices received by FESS directly or from internal department emails	Invoices are being sent directly to departments, resulting in slower processing
Payment analysis for same dollar amounts paid to same vendor via AP and GNWT credit card	Duplicate payments are being made
Timing of Payments	Payments are not being made in a timely manner
Comparison of PSS contract list for period tested with SAM contracts list for same period	Contracting is undertaken without the involvement of PSS, or without PSS' knowledge
AP Voucher payments over 10k	Payments are made in departments which should be made by FESS
Payment Authority Listing	Payment authority may be unnecessarily high introducing the risk that the approver may not understand or be aware of the goods acquired or services received prior to ultimate payment being authorized
List of available training in regards to the P2P cycle	Training is not adequate to address risk of incorrectly handled procurement and payment

It should be noted that IAB's ACL data analytic software was utilized as part of this audit to enhance testing of full data sets versus placing reliance on sample testing only.

APPENDIX H: VALUES AND GUIDING PRINCIPLES OF PUBLIC PROCUREMENT

Accountability

Taking ownership and being responsible to stakeholders for our actions...essential to preserve the public trust and protect the public interest.

- **Principles:**
 - Apply sound business judgment.
 - Be knowledgeable of and abide by all applicable laws and regulations.
 - Be responsible stewards of public funds.
 - Maximize competition to the greatest extent practicable.
 - Practice due diligence.
 - Promote effective, economic, and efficient acquisition.
 - Support economic, social, and sustainable communities.
 - Use procurement strategies to optimize value to stakeholders.

Ethics

Acting in a manner true to these values...essential to preserve the public's trust.

- **Principles:**
 - Act and conduct business with honesty and integrity, avoiding even the appearance of impropriety.
 - Maintain consistency in all processes and actions.
 - Meet the ethical standards of the profession.

Impartiality

Unbiased decision-making and action...essential to ensure fairness for the public good.

- **Principles:**
 - Be open, fair, impartial, and non-discriminatory in all processes.
 - Treat suppliers equitably, without discrimination, and without imposing unnecessary constraints on the competitive market.
 - Use sound professional judgment within established legal frameworks to balance competing interests among stakeholders.

Professionalism

Upholding high standards of job performance and ethical behavior...essential to balance diverse public interests.

- **Principles:**
 - Be led by those with education, experience, and professional certification in public procurement.
 - Continually contribute value to the organization.
 - Continually develop as a profession through education, mentorship, innovation, and partnerships.
 - Develop, support, and promote the highest professional standards in order to serve the public good.
 - Seek continuous improvement through on-going training, education, and skill enhancement.

Service

Obligation to assist stakeholders...essential to support the public good.


- **Principles:**
 - Be a crucial resource and strategic partner within the organization and community.
 - Develop and maintain relationships with stakeholders.
 - Develop collaborative partnerships to meet public needs.
 - Maintain a customer-service focus while meeting the needs, and protecting the interests, of the organization and the public.

Transparency

Easily accessible and understandable policies and processes...essential to demonstrate responsible use of public funds.

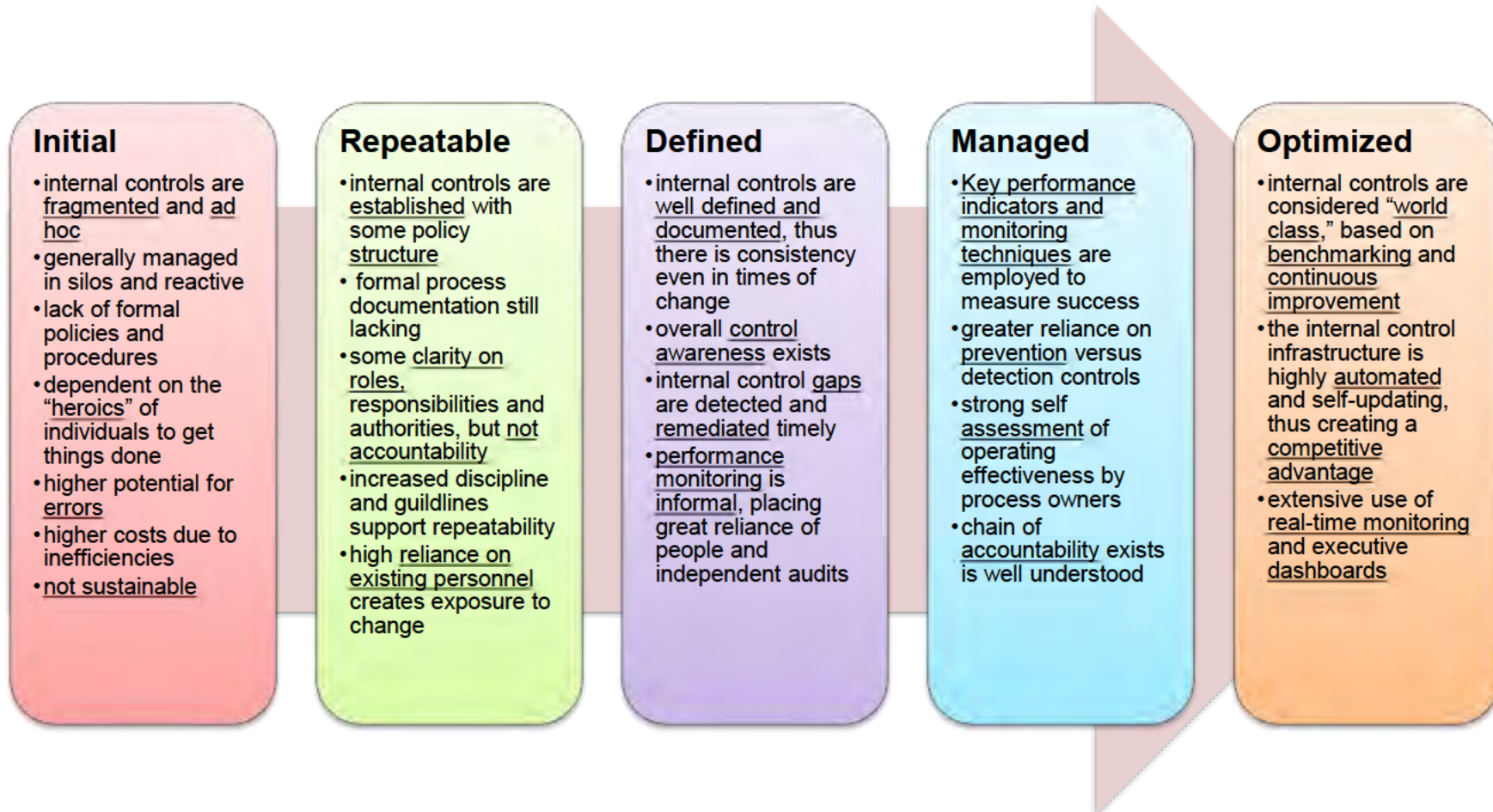
- **Principles:**
 - Exercise discretion in the release of confidential information.
 - Maintain current and complete policies, procedures, and records.
 - Provide open access to competitive opportunities.
 - Provide timely access to procurement policies, procedures, and records.

National Institute of Governmental Purchasing, October, 2010

 Northwest Territories	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: APPENDIX I: INTERNAL CONTROL CAPACITY MODEL		Task Number: 153

Deliverable	Description
0 - Non-existent	<ul style="list-style-type: none"> • The organization lacks procedures to monitor the effectiveness of internal controls. • Management internal control reporting methods are absent. • There is a general unawareness of internal control assurance. • Management and employees have an overall lack of awareness of internal controls.
1 - Initial/Ad Hoc - Unreliable	<p>Unpredictable environment for which controls have not been designed or implemented.</p> <ul style="list-style-type: none"> • Controls are fragmented and ad hoc. • Controls are 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 and higher costs due to inefficiencies. • Controls are not sustainable. • Individual expertise in assessing internal control adequacy is applied on an ad hoc basis. • Management has not formally assigned responsibility for monitoring the effectiveness of internal controls.
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"> • Controls are established with some policy structure. • Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. • Formal process documentation is still lacking. • Some clarity on roles and responsibilities, but not on accountability. • Increased discipline and guidelines support repeatability. • High reliance on existing personnel creates exposure to change. • Internal control assessment is dependent on the skill sets of key individuals.
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"> • Controls are well-defined and documented, thus there is consistency even in times of change. • Overall control awareness exists. • Policies and procedures are developed for assessing and reporting on internal control monitoring activities. • A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers. • Control gaps are detected and remediated timely. • Performance monitoring is informal, placing great reliance on the diligence of people and independent audits • Management supports and institutes internal control monitoring. • An education and training program for internal control monitoring is defined.

Deliverable	Description
	<ul style="list-style-type: none"> Tools are being utilized but are not necessarily integrated into all processes.
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"> Key Performance Indicators (KPIs) 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 and is well-understood. Management implements a framework for internal control monitoring. A formal internal control function is established, with specialized and certified professionals utilizing a formal control framework endorsed by senior management. Skilled staff members are routinely participating in internal control assessments. A metrics knowledge base for historical information on internal control monitoring is established. Peer reviews for internal control monitoring are established. Tools are implemented to standardize assessments and automatically detect control exceptions.
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"> Controls are considered “word class, based on benchmarking and continuous improvement. The control infrastructure is highly automated and self-updating, thus creating a competitive advantage. Extensive use of real-time monitoring and executive dashboards. Management establishes an organization wide continuous improvement program that takes into account lessons learned and industry good practices for internal control monitoring. The organization uses integrated and updated tools, where appropriate, that allow effective assessment of critical controls and rapid detection of control monitoring incidents. Benchmarking against industry standards and good practices is formalized.



APPENDIX J: AUDIT RISK ASSESSMENT HEAT MAP

(A) Likelihood	(B) Impact					(C) Overall Risk:	
	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Extreme		
5. Almost Certain	6	7	8	9	10	Very High	9 to 10
4. Likely	5	6	7	8	9	High	8
3. Possible	4	5	6	7	8	Medium	5 to 7
2. Unlikely	3	4	5	6	7	Low	4
1. Rare	2	3	4	5	6	Very Low	1 to 3

(A) Likelihood of Risk

Likelihood of Risk	Criteria
5 – Almost Certain	Event has occurred in the last 2 years and/or likelihood to happen in the next 3 to 5 years is high (>75%)
4 – Likely	Event has occurred in the last 5 years and/or it could happen again in the next 3 to 5 years (50% to 75%)
3 – Possible	Has occurred in the last 7 years and/or likelihood to happen in the next 3 to 5 years is moderate (25 to 50%)
2 – Unlikely	Has occurred in the last 10 years and/or the likelihood of it happening is moderate (not higher than 25%)
1 – Rare	Has not happened in more than 10 years and/or is not likely to occur in the next 3 to 5 years (<10%)

(B) Overall Risk

The overall risk is calculated using the following formula:

- Likelihood + Impact (Damages & Liabilities *30% + Operational Effect * 20% + Reputation *50%)
- Round up the value

For example: a likely event [4] + with a Major Damage & Liability impact [4*.3] + an Insignificant Operational Effect [1*.2] + and Moderate Reputation impact [3*.5] will result in overall score of 6.9. This would be rounded up to 7 for Overall Risk of Medium.

(C) Impact Measurement Tool - Corporate Level

Impact Level	Damages and Liability (30%)	Operational Effects (20%)	Reputation (50% Weight)
5 Extreme Managed by Senior Management with detailed plans	18(a)		
4 Major Require detailed research and planning by Senior Management			
3 Moderate Require specific allocation of management responsibility			
2 Minor Requires management through specific, monitoring or response procedures			
1 Insignificant Can be managed by routine procedures			

	<ul style="list-style-type: none">• Very minor, non-permanent environmental damage requiring no clean-up measures	<ul style="list-style-type: none">• Additional revenue of less than \$100,000	
--	---	---	--

APPENDIX L: GENERAL OBSERVATIONS FOR MANAGEMENT CONSIDERATION

A: Procurement

Listed below are observations of lower risk relating to the area of procurement noted during audit work. Recommendations have been made for management's consideration.

Observation 1

SAM issues with doubling sole source amounts.

When a multi-year Sole Source contract is set up and coding is split between two department areas, the system automatically doubles the sole source amount. If this is not noted, the commitment to that contract will be higher than budgeted by the department and could lead to inaccurate accounting. Feedback from the SAM team to the departments suggests that this is not an issue that can be fixed.

Opportunities for Improvement:

We recommend that:

- a) Further review be performed to ensure this cannot be addressed by Oracle.
- b) If this can't be corrected, it is essential that all staff members working in procurement be made aware of the issue so they will be alert to the risk of incorrect entry. A written notification should be provided from IT to all departments noting this issue and how to appropriately deal with it.

Management Response: Doubling sole source amounts cannot be addressed by Oracle as this is not a software issue. This only occurs on a multi-year sole source contracts. ERPS will work with PSS to ensure the correct SAM steps are documented and sent out to procurement staff. ERPS will include these steps in our standard eProcurement training.

B) Contract Management

Listed below are observations of lower risk relating to the area of contract management noted during audit work. Recommendations have been made for management's consideration

Observation 2

WSCC Clearance responsibilities are misunderstood.

A consistent issue noted with the review of files was the lack of up to date WSCC clearance letter on file. This was noted both at the PSS level and in the departments selected for testing. Through Crowe's interviews with each department it was noted that there is confusion by the departments as to who is responsible for obtaining both the WSCC clearance letter as well as required insurance documents. Confusion also extended to the department's lack of understanding of their roles and responsibilities for multi-year contracts, that point where the initial contract is handed by PSS to the department for ongoing monitoring and management.

Opportunities for Improvement:

We recommend that:

- a) The Service partnership agreement be updated to agree with the Procurement Guidelines to provide a consistent message to all parties involved in the P2P cycle as related to contract management.
- b) Clear communication be made to all departments as to their specific roles in the ongoing management of contracts.

Management Response:

- a) The partnership agreements are currently being updated. (March 31, 2020)

b) PSS have clearly communicated to departments as to their specific roles related to ongoing contract management since the implemented of PSS. This information is clearly outlined and communicated to client departments through:

- Contact Management workshops
- How to work with PSS workshops
- In PSS businesses process, that are available to client departments
- In the contract information package that is sent to client departments

Once the contract is awarded, the client is responsible for managing all aspects of the contract. It should be mandatory that any GNWT official responsible for managing contracts, take the contract management workshop.

Observation 3

Safety orientation minutes, checklists and evaluations were missing from files.

As noted in the Department findings above, it was noted that there were safety orientation minutes, checklists and evaluations missing from a number of different files. Although safety processes and procedures are outside the scope of this audit, and the testing was specific to certain departments, it should be noted that safety is always a high risk area and steps should be taken by all departments to ensure that when applicable, this type of documentation is clearly noted and maintained in each contract file.

Opportunities for Improvement:

We recommend that:

- a) Departments ensure all staff members involved in procurement are reminded of the need to assess contracts to determine if safety processes are required, and if so, understand the need for clear and concise documentation to be kept on file.

Management Response:

This will be addressed through ongoing contract management training.

C) Payment

Listed below are observations of lower risk relating to the area of payment noted during audit work. Recommendations have been made for management's consideration

Observation 4

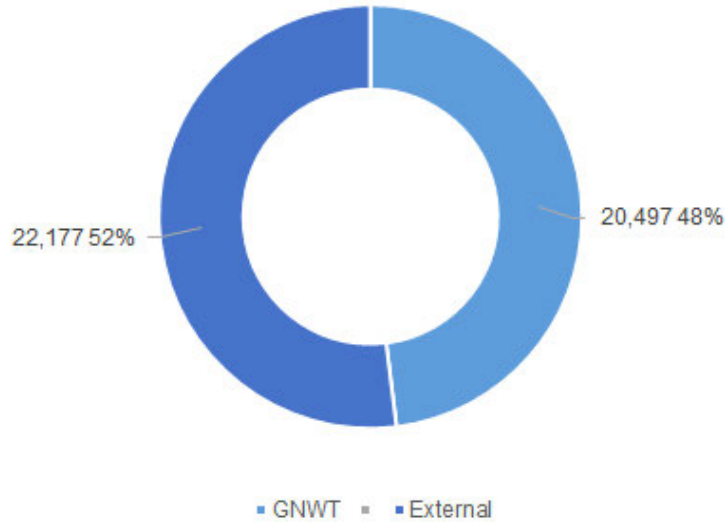
Duplicate payments are occurring, and additional fees are being charged.

DIIMS Workflow Email Comparative

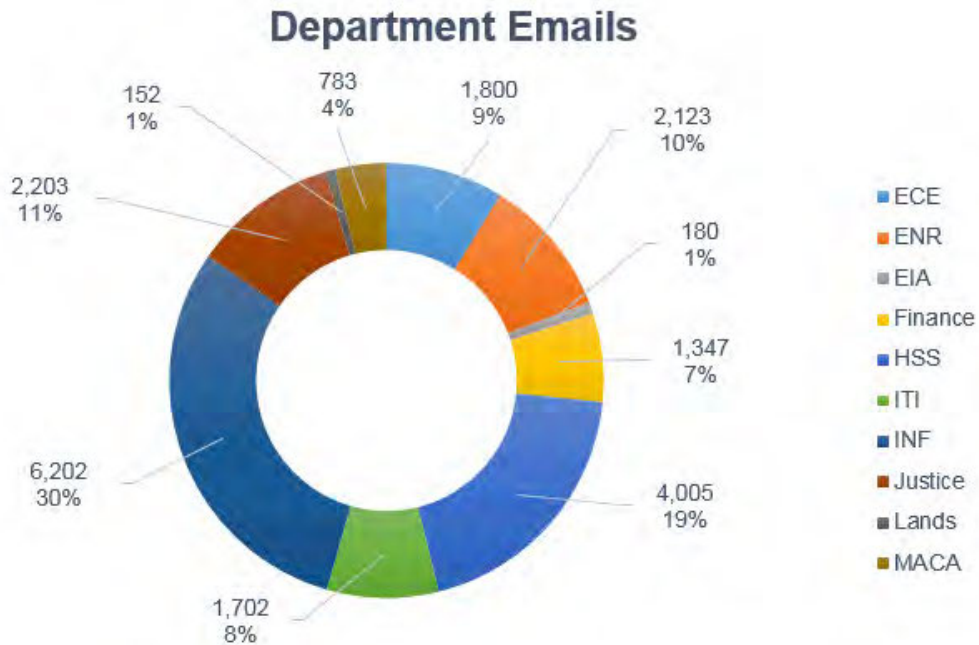
DIIMS workflow data was obtained and reviewed to determine the extent of invoices received by departments from vendors and then transferred to FESS for processing. This was completed by identifying the source of each email, whether received from an external email address (i.e. vendor) or from an internal email address (i.e. department). To adjust the data evaluated, any emails received from internal addresses related to FESS as well as NWTHC were removed from the population.

The current procedure is for invoices to be received by FESS directly from the vendor. The workflow data allowed Crowe to evaluate only the number of emails received to a central email address at FESS and not to other email addresses within the shared services group or whether single or multiple invoices were attached to those emails. While the evaluation did not allow for an opinion on the full process, it did identify sufficient evidence to conclude that treatment of invoices, and the GNWT's communication with each vendor, is not adequately addressing the need for invoices to be sent directly to FESS versus the individual department. A summary of the results are as follows:

DIIMS Workflow Email Comparative



The analysis suggested that overall, there are significant numbers of invoices coming via internal transfer from the departments to FESS. During our interviews with the departments, each validated this finding commenting that invoices continue to be received directly at the department level versus being submitted to FESS for processing. Not only is this process inefficient for GNWT resources, it also raises the risk of both duplicate payment as well as the potential for late payment of invoices. A breakdown of emails by department is as follows



Duplicate Payment Analysis

Data analytics were conducted to ascertain the risk of duplicate payments. Parameters utilized evaluated payments made by GNWT for the same amount, on the same date, and to the same vendor. This assessment was looking for the risk that an Accounts Payable (AP) voucher was processed and paid by FESS while simultaneously an invoice was paid directly by a department with a GNWT credit card. The data set obtained and tested was received from SAM for the period of April 1, 2018 to January 31, 2019. 20 individual payments were noted as possible duplicates. Further testing was performed on 3 vendors to which duplicate payments appeared to have been made. The total of payments made to the vendors was \$24,192 (1 duplicate to two vendors, and 3 duplicates for one vendor); these payments were all confirmed to be duplicate payments. Each transaction was approved by the same expenditure authority. As outlined above with the treatment of invoices received by departments, FESS, or both, the risk of duplicate payment did come to fruition.

Under the FAM, all invoices less than \$10,000 that do not have a corresponding PO are to be paid by the department. Payment at the department level can be transacted one of two ways:

- Purchases are paid by GNWT credit card at point of sale; invoices for these purchases are never sent to FESS and are kept by the cardholder to include with the monthly credit card reconciliation.
- Invoices received by FESS that are pushed to the department to pay:

Issues that arise with this process are as follows:

- Duplicate payments are occurring because the invoice is sent to both FESS as well as the respective department. The department staff process payment on GNWT credit card where the transaction is less than \$10,000. FESS will send the invoice to the department for processing and the department pays the same invoice again.
- Per discussions with department representatives during fieldwork, it was noted that some department staff members ask for a copy of the invoice to be sent to them so that they can ensure payment takes place. Having that additional copy in the department can also increase the risk that payment is made in the department as well as by FESS.
- Invoices received by FESS and sent to department(s) for processing through GNWT credit card miss the opportunity to withhold payment should the vendor have a balance owing to the GNWT.
- Some vendors have introduced administration fees for transactions processed on GNWT credit cards. This has increased the cost of procurement activities under \$10,000 to the GNWT as a whole. Where departments are attempting to avoid this additional cost, invoices are being sent back to FESS for processing which is increasing both confusion as well as inefficiencies. Additional time to process payment can also create extended delays which now introduces interest expense. Extending the timeline for payment also breaches the expectations set out in the FAM for payment processing.

Opportunities for Improvement:

We recommend that:

- a) All point-of-sale transactions should be paid on GNWT credit card. The GNWT should reevaluate the threshold at which a GNWT credit card should not be used for individual transactions by understanding the typical value of point-of-sale transactions historically. All invoices generated by vendors should be sent to FESS for processing regardless of the amount of the invoice. This process change would reduce the risk of duplicate payments as well as inefficiency for moving invoices between vendors and departments/FESS.
- b) Clear guidance should be updated and provided to vendors transacting with the GNWT which mandate that all invoices be submitted to FESS for payment. Where invoices are received by a department, they are to be returned directly to the vendor with instruction/reminder provided. Department staff should not be requesting additional copies of invoices.

Management Response: A vendor communication plan is in draft to clarify how vendors should be communicating with the GNWT, including submitting invoices. Draft kick-off date is Fall 2019.

Observation 5

Slow turn-around times for vendor setup

Feedback from departments suggested that an area of concern in relation to FESS processing was the time it takes for vendor setup to take place.

Opportunities for Improvement:

We recommend that:

- a) A review be performed with management from FESS to assess the time that it takes to process vendor setup and determine where there may be inefficiencies. These should then be addressed through specific steps.

Management Response: Vendor set-up times are included in the service level standards which departments were consulted on throughout the winter 2019. Reporting on service level standards targets will begin in July 2019.

Observation 6

No process in place for addressing purchasing authorities when staff transfer between departments.

During departmental interviews Crowe determined that processes are deemed rigorous for adding/adjusting/removing purchasing authorities for new and/or terminated employees. However, processes were not rigorous for making these same adjustments for staff transferring between departments. Some staff still had their authorities from previous departments and could transact on their behalf even though they no longer had any responsibilities within those respective departments.

Opportunities for Improvement:

We recommend that:

- a) Processes be developed and checklists made to ensure transfers between departments have their authorities reviewed and adjusted in a timely manner. The new department is to provide the correct authorities for the new position while the old department is to ensure authorities are removed.

Management Response: ERPS processes SAM Security access forms when received. This is an on-boarding / off-boarding issue not a SAM system issue. SAM access reports are reviewed monthly and signed off quarterly by Departmental DFAs.

Observation 7

Default Coding

Data for the analysis for default coding can only be obtained when requested and is not routinely stored for reporting and/or analysis. This data was requested to ascertain the number of default coded items and whether the number is static, increasing or decreasing. Results from both requests are as follows:

February 28, 2019	214 items noted with default coding
March 11, 2019	226 items noted with default coding

As expected, per review of the detailed data, the largest number of items related to INF, and this is due to the fact that the large majority of P2P payments goes through this department, and they manage a large number of construction contracts which may be of a more complex nature. Based on the sheer volume of invoices going through FESS each month, the default coding does not appear to be excessive.

Per the interview process with departments, it was asked whether or not the departments felt that default coding was excessive, or an issue. The vast majority of departments felt the process was reasonable and

that items were default coded when it was truly difficult to determine where it applied based on the information provided by the vendor. No recommendations have been made in relation to this observation.

Observation 8

PO Match exceptions not fully monitored and resolved

This report is run to identify whether vouchers from the current fiscal period have errors related to the following two conditions:

- 1) The PO is from the prior year and has not been updated (i.e. annually PO numbers are required to be updated and cannot continue with the same number for more than one year); and
- 2) There are no funds remaining in the PO for which to pay the voucher.

Match exception reports are important as disbursements are not permitted by the FAA unless there is money available for the purpose for which the disbursement was intended. Without a PO that matches, payment would be processed in contravention of the FAA.

Data requests to conduct this analysis cannot be obtained through setting a beginning and end date for the period to be reviewed. Rather, it can only be run as/when requested and will include any/all exceptions in existence as at that particular date. Crowe discussed historic data requests with FESS and noted they had obtained data as at October 2, 2018 (obtained from FESS). In addition to this date, Crowe also made another request as at March 5, 2019.

114 exceptions were identified in the October 2018 report with a total of 254 exceptions identified in the March 2019 report. Details of each report were compared to determine whether all exceptions had been cleared or whether stale dated items existed (i.e. exceptions stayed in “unmatched status” from October to March). The results of the comparison were as follows:

Department	Voucher Count
ENR	7
FIN	10
ITI	1
Total	18

This depicts delays in follow-up by the respective departments to clear identified exceptions. FESS cannot process payment of the vouchers until they are cleared by the department.

Exceptions exist and continue to stay outstanding for extended periods of time (i.e. 6 months for the reporting period denoted above). FAM 720 specifies payment processing timelines. Exceptions not cleared by departments may eventually breach FAM guidelines which requires payment within a maximum of 30 days.

Opportunities for Improvement:

We recommend that:

- a) FESS provides a complete list of match exceptions to each department (as applicable) on a monthly basis, including an agreed to timeline for departmental response and appropriate exception actioning.
- b) Each department create a new procedure to require monthly exception report monitoring with exceptions cleared in a timely manner. This will include coordination with FESS.

Management Response: FESS will work with the DFA Committee to review appropriate action.

Observation 9

Utilities have an exception to the \$10,000 limit, but similar payments do not.

FESS makes exceptions to the \$10,000 GNWT credit card rule for utilities. There are other payments that are utility-like in that regular payments are made routinely and that there is high risk of duplicate payments with these invoices going to both departments and FESS (as noted above). Two bills that are a problem for departments are Northwest Tel bills and the bills for photocopiers, i.e. Xerox/Ricoh.

Opportunities for Improvement:

We recommend that:

- a) Consideration be made to add Northwest Tel, Xerox and Ricoh bills to the exception listing.

Management Response: Effective June 2019 Northwest Tel bills will be added to the utilities exception list. FESS engaged in a discussion with PSS on Ricoh bills and it was determined that due to the purchase order tracking on this vendor that Ricoh invoices cannot be paid by VISA. FESS confirmed with Xerox that they will not accept VISA payments for invoices over \$200, and Xerox has been added to the list of vendors that take VISA for bills under \$200.