TD 774-19(2) TABLED ON NOVEMBER 1, 2022

Government of Northwest Territories | Gouvernement des Territoires du Nord-Ouest

**CONFIDENTIAL**

March 29, 2021

File: 7820-20-INF-151-100

MR. STEVE LOUTITT
DEPUTY MINISTER
INFRASTRUCTURE

**Audit Report:** **Department of Infrastructure Airports Division Safety Management System Triennial Audit**

**Review Period:** **April 1, 2018 to December 31, 2020**

## A. SCOPE AND OBJECTIVES

At the request of the Department of Infrastructure (INF), the Audit Committee approved the triennial audit of INF Airport Safety Management System's (INF SMS) compliance with *Canadian Aviation Regulations (CARs)*.

## B. BACKGROUND

The Transport Canada's *Aeronautics Act* required that all certified airports comply with CARs. The GNWT had 27 airports, 20 were certified by Transport Canada and 7 were registered (**Appendix A refers**).

Airports were certified under Subsection 302.03 of CARs. To ensure compliance, CARs Subsection 302.503 required the holder of an airport certificate to have a Quality Assurance Program (QAP). The QAP includes periodic audits of the activities authorized under the airport certificate. CARs required that each airport be audited once every three years. INF conducted a series of audits over the 3 years covering all 20 NWT airports.

SMS was a documented system for managing risks to ensure the safety of the public. QAP was the internal validation function of SMS ensuring that SMS was effective, being adhered to, and any non-compliance were analyzed and corrected.

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

## C. INDEPENDENT ASSESSMENT

We examined the documents and records that supported the QAP. Based on the information gathered and the explanations given to us, INF SMS was generally in compliance to CARs except for the following:

- The Corrective Action Plans (CAPs) for Yellowknife airport, which was due on June 15, 2020, had not yet been submitted as of March 9, 2021 **(Appendix B refers)**. CARs 302.505(1)(a)&(e) required the timely collection of information related to hazards, incidents, and accidents; and, the evaluation and monitoring of corrective actions with respect to those hazards, incidents, and accidents.
- The CAPs for Wekweeti, Lutselke, and Fort Simpson airports were submitted after the 30 days threshold for CAPs submission specified in INF SMS Manual **(Appendix B refers)**.
- 100% of our risk-based samples (5 of 16 airports) exceeded the 90 days threshold for implementing and closing out CAPs specified in INF SMS Manual. Noncompliance ranged from 8% to 77% **(Appendix C refers)**.
- Onsite visits, scheduled to commence in October 2020 for the four Sahtu region airports, did not occur due to COVID. Other INF personnel traveling from Yellowknife to communities for unrelated work were requested to perform some audit procedures. Due to time constraint, those personnel were not able to carry out the request. The airport manager's inspection reports were relied upon instead. The audit team planned to conduct follow-up onsite inspections at a later date.
- CARs 302.503(3)(e) required that each audit finding be reported to Accountable Executive (or Deputy Minister of Infrastructure). INF SMS Manual and QA Audit Process Document had no provision for such requirement. The escalation to report QA audit findings stopped at the Assistant Deputy Minister.

We recommend that Transport Canada be consulted for the potential impact of the exceptions noted above.

We would like also to thank INF SMS staff for their assistance and co-operation during the audit.

T. Bob Shahi
Director, Internal Audit Bureau
Finance

**Appendix A**

**Infrastructure**
**2018-INF- Airport Safety Management System**
**File No. 7820-20-INF-151-100**
**April 1, 2018 to December 31, 2020**

## NWT Airports
## NWT Airports as of December 31, 2020

| **Certified Airports** | | | | **Registered** | |
|---|---|---|---|---|---|
| **"A" Airports** | **Region** | **"B" Airports** | **Region** | **Registered** | **Region** |
| Inuvik | Beaufort Delta | Aklavik | Beaufort Delta | Fort Liard | Deh Cho |
| Norman Wells | Sahtu Region | Fort McPherson | Beaufort Delta | Jean Marie River | Deh Cho |
| Fort Simpson | Deh Cho | Paulatuk | Beaufort Delta | Nahanni Butte | Deh Cho |
| Yellowknife | North Slave | Sachs Harbour | Beaufort Delta | Trout Lake | Deh Cho |
| Fort Smith | South Slave | Tuktoyaktuk | Beaufort Delta | Wrigley | Deh Cho |
| Hay River | South Slave | Ulukhaktok | Beaufort Delta | Fort Providence | South Slave |
| | | Colville Lake | Sahtu | Fort Resolution | South Slave |
| | | Deline | Sahtu | | |
| | | Fort Good Hope | Sahtu | | |
| | | Tulita | Sahtu | | |
| | | Gameti | North Slave | | |
| | | Lutselk'e | North Slave | | |
| | | Wekweeti | North Slave | | |
| | | Whati | North Slave | | |
| 6 | | 14 | | 7 | |
| **Total number of Airports** | | | | 27 | |

### Certified Airports

A= Have paved runways and managed by GNWT staff.

B= Have Gravel runways and managed by contractors usually municipal Governments.

**Registered** = Airports with no scheduled traffic were not required by Transport Canada to have a Safety Management System.

**Appendix B**

## Infrastructure
## 2021-INF-Airport Safety Management System
## FILE NO: 7820-20-INF-151-100
## April 1, 2018 to December 31, 2020

### Corrective Action Plans (CAPs) non-compliant to 30-day requirement per SMS Manual Sec. 3.9

| Airport<br>(A) | Submission Due Date given by SMS Manager<br>(B) | Submission Date by Airport Management<br>(C) | Days Lapsed<br>(D)<br>[c – b] |
|---|---|---|---|
| Yellowknife (**NOTE 1**) | Jun/15/2020 | [redacted] | [redacted] |
| Wekweeti (**NOTE 2a**) | Aug/15/2019 | Nov/9/2020 | 452 |
| Lutselke | Oct/20/2018 | Feb/18/2019 | 132 |
| Fort Simpson (**NOTE 2b**) | May/18/2018 | Jul/01/2018 | 44 |
| Fort Smith | Aug/25/2018 | Aug/30/2018 | 5 |

**NOTES:**

1. As of March 9, 2021, Yellowknife airport had not yet developed and submitted its Corrective Action Plans

2. As allowed by Section 3.9 of the INF SMS Manual, extensions on CAPs submission due dates were requested by the airport management of:

   a. Wekweeti: Extend its due date from August 15, 2019 to:
      - 1st – August 23, 2019
      - 2nd – September 27, 2019
      - 3rd – November 22, 2019
      - 4th – December 5, 2019

   b. Fort Simpson: Extend its due date from May 18, 2018 to June 1, 2018.

**Appendix C**

# Infrastructure
## 2021-INF-Airport Safety Management System
## FILE NO: 7820-20-INF-151-100
## April 1, 2018 to December 31, 2020

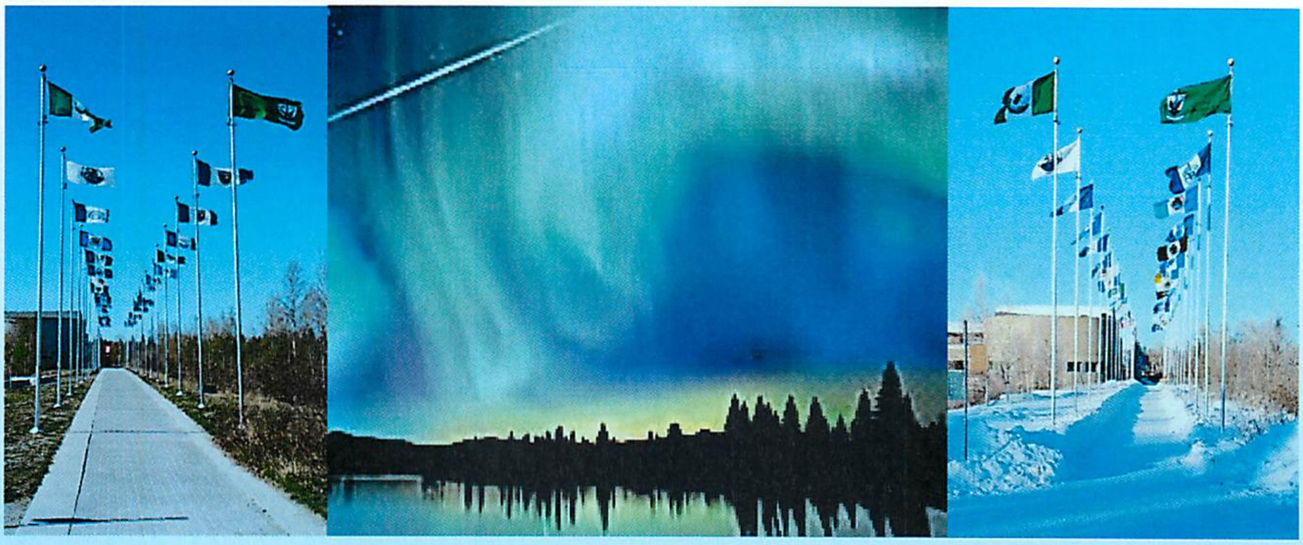
### Corrective Action Plans (CAPs) non-compliant to 90-day requirement per SMS Manual Sec. 3.9

| Airport (A) | CAPs Approval Date (B) | CAPs Completion Date Range (C) | Total Number of CAPs (D) | Total Noncompliant CAPS (E) | Non-Compliance % (F) [e / d] |
|---|---|---|---|---|---|
| Yellowknife **(NOTE 1)** | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |
| Fort Simpson | Jul/1/2018 | Jul/18/2018 to Oct/05/2020 | 28 | 17 | 61% |
| Fort Smith | Aug/30/2018 | Aug/3/2018 to Feb/2/2020 | 3 | 2 | 67% |
| Lutselke | Mar/1/2019 | Feb/18/2019 to Dec/03/2020 | 13 | 10 | 77% |
| Wekweeti **(NOTE 2)** | Nov/9/2020 | Oct/07/2020 To Feb/11/2021 | 38 | 3 | 8% |

**NOTES:**

1. Yellowknife airport has not submitted its CAPs as of March 9, 2021; thus, approval and completion of CAPs were not applicable
2. Wekweeti airport's three non-compliant CAPs didn't have a completion date as of March 9, 2021, the date this analysis was completed.

Government of Northwest Territories Gouvernement des Territoires du Nord-Ouest



# Transportation

## Audit of the Deh Cho Bridge Toll Revenue

Internal Audit Bureau – Audit Report
March 2017

# Audit Report
## Operational Audit

## Transportation
## Audit of the Deh Cho Bridge Toll Revenue

March 2017

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

Government of Northwest Territories
Gouvernement des Territoires du Nord-Ouest

**CONFIDENTIAL**

March 22, 2017

File: 7820-20-DOT-151-118

MR. RUSSELL NEUDORF
DEPUTY MINISTER
TRANSPORTATION

**Audit Report: Audit of the Deh Cho Bridge Toll Revenue**
**Audit Period: April 1, 2015 – January 31, 2016**

## A. SCOPE AND OBJECTIVES

The Audit Committee approved the Department of Transportation (DOT) management requested audit of the Deh Cho Bridge (Bridge) toll revenue for the 2015-2016 audit work plan. The audit objectives were to determine if:

- the governance framework was clear, understood, and current to allow the DOT staff and management to collect all eligible Bridge toll revenue.
- Bridge toll revenue information was relevant, reliable, accurate, complete and timely to allow the DOT to manage the toll revenue collection.
- Bridge toll revenue processing complied with the *Deh Cho Bridge Act* (the Bridge Act), Deh Cho Bridge Regulations (Regulations), Bridge Toll Remittance Agreement, *Access to Information and Protection of Privacy Act* (ATIPP), Financial Administration Act, Financial Administration Manual (FAM), and the Visual Identity Program.
- the Bridge gantry and toll revenue was safe, secure, and accounted for.
- adequate controls were in place for the effective and efficient processing of Bridge toll revenue transactions.
- Business continuity plans and related controls covering people, process, and technology were appropriate to support DRIVES over the next three to five years; and
- the vendor, Winding River Solutions had an appropriate internal control capacity to support DRIVES over the next three to five years.

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

## B. BACKGROUND

*The Bridge Act* requires all registered owners of northbound commercial vehicles weighing over 4,500kg to pay a toll to cross the Bridge. For the period of April 1, 2015 to January 31, 2016, nearly 13,000 northbound commercial vehicles weighing over 4,500kg crossed the Bridge, and over $3.1M in actual revenue was reported as collected. All transactions and operations related to the Bridge tolling during the above noted time period were considered within the audit scope.

The audit contract was awarded to Grant Thornton by a Request of Proposal evaluation team composed of DOT and Internal Audit Bureau (IAB) staff.

## C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The attached audit report by Grant Thornton made a number of observations pertaining to the audit objectives. Management has already taken action to address some items, and has accepted the risk of the existing conditions for some others.

Positive observations included:

1) There were automated controls within DRIVES which helped reduce the risk of lost revenue and improved the efficiency of the Tolling Matchup process.
2) DRIVES access used a secured integrated authentication with a central directory.
3) The developer of DRIVES, Winding River Solutions, had the depth and capacity to meet the development requirements of the system.

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

1) Finalizing the Toll Procedures Manual and updating the help function in DRIVES.
2) Implementing a process to detect misclassified events resulting in no revenue.
3) Enforcing fines for bypassing the Bridge toll, improving document management practices, formal disclosure of the required ATIPP policies to carriers, and assurance that follow-ups on receivables are completed in accordance with FAM.

4) Enhancing the identity and access management controls & processes for DRIVES.
5) Enhancing user awareness of the accounts receivable information available in SAM, and implementing a tracking tool for issues resulting from the automated matching process.
6) Conducting a formal business impact assessment, developing & implementing a formalized recovery plan, business continuity plan, and a disaster recovery plan.
7) Updating the contract with Winding River to ensure that the GNWT and DOT have complete access to the full suite of system documentation.

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

## D. ACKNOWLEDGEMENT

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

T. Bob Shahi
Director

Grant Thornton
An instinct for growth™

# Government of the Northwest Territories

## Department of Transportation

## Audit Report

# Audit of the Deh Cho Bridge Toll Revenue

March 2016

## TABLE OF CONTENTS

# 1.0 EXECUTIVE SUMMARY

## 1.1 Background / Context

In January 2016, the Government of Northwest Territories (GNWT) engaged Grant Thornton LLP (GT) to conduct an Operational Audit of the Deh Cho Bridge (the Bridge) toll revenue process, performed by the Department of Transportation (the Department or DOT). As part of this audit, procedures were requested to be conducted on the toll revenue process. GNWT uses DRIVES as its motor vehicle information system and System for Accountability & Management (SAM) is the financial system used by DOT.

The Northwest Territories Deh Cho Bridge Act (the Act) requires all registered owners of northbound commercial vehicles weighing over 4,500 kg to pay a toll to cross the Bridge. Private, service and commercial vehicles weighing less than 4,500 kg are exempt from paying the toll fees.

For the period of April 1, 2015 to January 31, 2016 the number of northbound commercial vehicles weighing over 4,500 kg that crossed the Bridge and the toll revenue collected is listed in the table below (information in the table below was provided by DOT):

| Period | # of Vehicles (A)<br>(Per DRIVES raw data[1]) | Actual Revenue (B)<br>(Per DRIVES Toll Reconciliation[2]) | Average $ per crossing<br>(C = A / B) |
|---|---|---|---|
| April 1, 2015 to January 31, 2016 | 12,998 | $3,121,927 | $240 |

## 1.2 Audit Objectives and Scope

The objectives of the operational audit were to determine if:

1. **Governance Framework** - The Act, regulations, policies, procedures and other relevant frameworks were clear, understood, and current to allow the Department staff and management to collect all eligible Bridge toll revenue
2. **Information integrity** - The Bridge toll revenue information was relevant, reliable, accurate, complete and timely to allow the Department's staff & management to collect and use the information to manage the revenue collection
3. **Compliance** - The processing of Bridge toll revenue was in compliance with the Act, Regulations, Bridge Toll Remittance Agreement, Access to Information and the Protection of Privacy Act, Financial Administration Act, Financial Administration Manual and Visual Identity Program
4. **Asset and Data Security** - The Bridge gantry and toll revenue was safe, secure, and fully accounted for
5. **Efficiency and Effectiveness** - There were adequate controls in place to allow for the effective and efficient processing of Bridge toll revenue transactions
6. **Business Continuity** - The business continuity plans and the related controls covering people, process, and technology are appropriate to support DRIVES over the next three (3) to five (5) years
7. **Vendor Management and Controls** - The vendor Winding River Solutions has an appropriate internal control capacity to support DRIVES over the next three (3) to five (5) years.

[1] DRIVES raw data – an extraction from DRIVES provided by the Manager, Information Systems

[2] DRIVES tolling reconciliation – a report GT extracted from DRIVES for all tolling events that generated revenue

Our audit scope covered the period from April 1, 2015 to January 31, 2016. All transactions and operations related to the Bridge tolling during that time period were considered within the audit scope.

## 1.3 Summary of Observations and Recommendations

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

The following positive observations were identified through the audit:

- There are automated controls within DRIVES which help reduce the risk of lost revenue and improve the efficiency of the tolling matchup process (Efficiency and Effectiveness)
- DRIVES access uses secured integrated authentication with a central directory (Asset and Data Security)
- The developer of DRIVES, Winding River Solutions, has depth and capacity to meet the development requirements of the system (Vendor Management and Controls)

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

| Audit Area | Key Observations | Impact Assessment | Report Section |
|---|---|---|---|
| 1. Governance Framework | ▪ Incomplete Tolling Procedures Manual | Minor | 2.2.1 |
| 2. Information Integrity | ▪ No review of events converted to categories that do not result in toll revenue (represents lost tolling revenue of approximately $62,200) | Moderate | 2.2.2 |
| 3. Compliance | ▪ Areas of non-compliance found with the Deh Cho Bridge Act, Access to Information and Protection of Privacy Act and Financial Administration Manual<br>▪ DRIVES is configured to allow for a 10% threshold for vehicle weight; therefore, vehicles between 4,500kg and 4,950kg do not result in toll revenue (represents lost tolling revenue of approximately $320,880) | High | 2.2.3 |
| 4. Asset and Data Security | ▪ Informal monitoring and controls over system access | High | 2.2.4 |
| 5. Efficiency and Effectiveness | ▪ Process and control inefficiencies identified | Minor | 2.2.5 |
| 6. Business Continuity | ▪ No formal Business Continuity Plan and Disaster Recovery Plan | Moderate | 2.2.6 |
| 7. Vendor Management and Controls | ▪ Gaps within contract terms and conditions with third party vendor identified | Moderate | 2.2.7 |

**Key Observations:**

**Objective 1: Governance Framework – Incomplete Tolling Procedures Manual**

In February 2015, DOT began developing a Deh Cho Tolling Procedures Manual (Tolling Procedures Manual or Manual) which is a comprehensive guide of the tolling process. The Tolling Procedures Manual contains an overview of each role (by level and name), associated responsibilities, expected outcomes, screenshots and visual instructions.

During our audit, the following observations were noted:

- For detailed procedures in the Manual, the responsible individual was not always identified
- Comments and questions were found in the Tolling Procedures Manual indicating that the final version may not be available to individuals responsible for the process steps

**Recommendation #1**

We recommend that DOT management:

- Finalize the Tolling Procedures Manual, include roles and responsibilities for all detailed procedures, and include all key processes (i.e. permit purchasing, semi-monthly reconciliation between DRIVES and the bank account, finance review of batch transactions, payment intake/processing, collections, accounts receivable processes, etc.)
- Update the help function to include the finalized Tolling Procedures Manual

**Objective 2: Information Integrity – Informal review of reconciliation variances, no review of some conversion categories and DRIVES configuration**

An event is defined as a vehicle that crosses the Bridge that may or may not be subject to a toll. There were 176,354 events per the DRIVES raw data[3] during our audit period. As part of the audit, tests were conducted on a random sample of 159 events (0.09% of all events) to assess the accuracy of classification. The audit test found that four (4) of 159 events tested were classified in the wrong category. The four (4) errors noted were in either the Exempt or Duplicate categories. The details on the four (4) errors were as follows:

- Exempt – The total population of Exempt events for the audit period was 1,293. Three (3) of the 30, or 10% of events tested in this category should not have been classified as Exempt. This represents potential lost revenues of $31,032[4].
- Duplicate – The total population of Duplicate events for the audit period was 583. One (1) of the 15, or 7% of events tested in this category should not have been classified as Duplicate. This represents potential lost revenues of $9,328[5].

The audit also assessed information integrity on the entire population of events (176,354). The following observations were noted:

- 58 of 176,354 events were converted to a status of "No Image/Image Unusable". For these events, either no pictures were captured by the system or the picture captured was not readable and therefore could not be used for matching. All of the 58 events were above the qualifying weight, which may represent lost toll revenue of up to $13,920[6].

[3] DRIVES raw data – an extraction from DRIVES provided by the Manager, Information Systems

[4] $31,032 = 10% error rate x 1,293 events x $240 average price (average price per crossing per pg.6 of the report)

[5] $9,328 – 7% error rate x 583 events x $240 average price (average price per crossing per pg.6 of the report)

[6] $13,920 = 58 events x $240 average price (average price per crossing per pg.6 of the report)

- 33 of 176,354 events were converted to a status of "No Match". For these events, DOT was unable to match an event to a carrier within DRIVES. All 33 events were above the qualifying weight, which may represent lost toll revenue of up to $7,920[7]. 15 of 33 events had pictures that clearly showed the license plate of the vehicle. Furthermore there is no documentation in DRIVES indicating the rational for converting these events to "No Match" status.

**Recommendation #2**

We recommend that DOT Management:

- Implement a risk-based review process that enables the detection of events that have been misclassified to a category that does result in a toll revenue. Higher risk events could include conversions to Exempt, Non-commercial, Image Unusable, No Image, Southbound, Duplicate and No Match
- In collaboration with the third party vendor that supports the bridge technology, conduct a review of the events that were deemed "No Image / Image Unusable" and determine the root cause of the image deficiency. Following the review, implement actions to help reduce the risk of the image deficiencies

### Objective 3: Compliance – Areas of non-compliance found with the Deh Cho Bridge Act, Access to Information and Protection of Privacy Act and Financial Administration Manual

The audit reviewed GNWT's compliance with a number of legislative and regulatory requirements related to the operations of the Bridge. Specifically this included; Deh Cho Bridge Act, Deh Cho Bridge Regulations, Financial Administration Act, Access to Information and Protection of Privacy Act, Financial Administration Manual and Visual Identity Program. The following observations of non-compliance were made regarding the above-noted regulations:

- **Deh Cho Bridge Act:** Fines were not imposed in accordance with the Deh Cho Bridge Act. During the audit testing period, it was found that 15 of the 33 events converted to "No Match" could be identified by a visible license plate. These vehicles crossed the Bridge without paying the appropriate toll and it was found that no fines were issued in these instances
- **Deh Cho Bridge Regulations:** The regulations require that an operator or registered owner of a commercial vehicle travelling northbound across the bridge pay a toll. Commercial vehicle means a motor vehicle used for business purposes that has a gross weight exceeding 4,500 kg. During the audit period, 158,935 of 176,354 events were converted to a status of "Below Qualifying Event Weight". It was found that 1,337 of the 158,935 events in this category were above 4,500 kg. Management indicated that DRIVES system is configured to allow for a 10% tolerance on vehicle weight. Therefore vehicles up to 4,950 kg would be automatically converted to a category that does not generate toll revenue. This practice is not in compliance with the regulations and may represent a potential for lost revenues of up to $320,880[8] if all events were for commercial vehicles.
- **Access to Information and Protection of Privacy Act:** The DOT is required to inform carriers of the purpose for collecting information, the legal authority for the collection and a contact person within the DOT. Through our review of the tolling website and the remittance agreement template, we did not observe this information being formally disclosed to the carriers
- **Financial Administration Manual:** The DOT is required to consistently review outstanding deliverables and take vigorous action on overdue receivables in accordance with the Financial Administration Manual. We selected three (3) carriers with AR balances between 91 – 120 days to test

[7] $7,920 = 33 events x $240 average price (average price per crossing per pg.6 of the report)
[8] $320,880 = 1,337 events x $240 average price (average price per crossing per pg.6 of the report)

whether follow ups were being performed on a timely basis. The results of our testing found that for two (2) out of three (3) carrier tested, there was no supporting documentation on follow up with the carrier

**Recommendation #3**

We recommend that DOT management:

- Enforce and issue fines for vehicles that cross the Bridge without paying the appropriate toll
- Review the existing DRIVES weight threshold and make required changes to ensure compliance with the regulations. In addition, implement an ongoing re-calibration of the scales to help ensure increased accuracy of weight measurement; DOT may wish to consider referencing relevant guidance published and set forth by Measurement Canada[9] in evaluating the configuration/recalibration of the weighing scale and practices in collecting revenue from weighing scales and stations
- Improve document management practices to help ensure remittance agreements with carriers are maintained and can be accessed in an efficient manner
- Formally disclose the required information to carriers regarding access to information and privacy
- Ensure that follow-up on receivables is conducted in accordance with the Financial Administration Manual requirements and documentation is maintained around follow-up actions

**Objective 4: Asset and Data Security – Informal monitoring and controls over system access**

We expected that access controls for DRIVES are adequately managed, appropriate, and documented. During our testing, we noted the following observations:

- There was no control or current capability to validate the authorization and approval of user access
- DOT has not established a process or controls to ensure privileges are appropriately assigned
- Several user account privileges did not support segregation of duty and least privilege principals
- Periodic review of accounts, access privileges and key transactions did not occur

**Recommendation #4**

DOT should take steps to review, update and enhance their overall Identity and Access Management controls and process for DRIVES. This would include the following:

- Conduct a full account review of DRIVES, validating access requirements, role assignment and privileges, ensuring that all accounts have the necessary authorization forms complete and that accounts are approved by an authorised representative. This review should identify accounts that are no longer used or are required to support DRIVES maintenance and support, such as the Winding River Solutions accounts. This review should be performed on an annual basis and supported through updated policies on account review
- Define an access control matrix for DRIVES that outlines baseline role and privilege assignment, conflicting roles, and plain descriptions of roles to guide the assignment of roles and privileges to users and groups
- Enhance the user account access and authorisation process to ensure that all user access requests have traceability, are formally authorised by appropriate supervisors or managers and have completed all the

[9] https://www.ic.gc.ca/eic/site/mc-mc.nsf/eng/Home

necessary background checks. This process and model should ensure that access requests capture the necessary details and identity data of a user and authorizer, including:

- Full name, email and contact details of requestor
- Role and title of requestor
- Requested level of access or system role (e.g. Examiner vs. Reviewer)
- Full name, email and contact details of requestor manager/supervisor (with demonstrated authority and approval of access request)
- Level of approved access or system role
- Term of access required and approved

- DOT should identify and maintain a baseline listing of installed equipment at the gantry, including device details and model numbers

### Objective 5: Efficiency and Effectiveness – Process and control inefficiencies identified

Through the conduct of the audit, process and control documentation was reviewed and walkthroughs were performed to determine whether process and controls were designed and operating in an efficient manner.

Although efficiencies were found throughout the process, opportunities were identified to further optimize the tolling process and controls. Specific examples include:

- Manual adjustments during the semi-monthly reconciliation may not be required given that all variances should be accounted for in the over/short account analysis that is performed at the end of the month
- Hay River Finance is tracking invoices and payments using a manual spreadsheet. Tracking and monitoring these amounts is a good practice, but this can be conducted through the SAM system. SAM can generate reports based on the information in the system, therefore these manual spreadsheets would not need to be used
- There is no tracking mechanism to follow-up on issues related to matching. Currently the Finance Administrative Staff, Finance Manager, Operations manager, Transport Compliance Manager and the Director of Road Licensing and Safety all follow up on issues related to matching

**Recommendation #5**

We recommend that DOT management:

- Explore the opportunity to remove manual adjustments to the semi-monthly reconciliation
- Enhance user awareness of the information, reports and functionality that can be generated from SAM with regards to accounts receivable management
- Implement a follow-up tracking mechanism for issues that arise from the automated matching process and identify specific individuals responsible for the follow-up procedures

### Objective 6: Business Continuity – No formal Business Continuity Plan and Disaster Recovery Plan

Key GNWT practices were reviewed to determine if the Office of the Chief Information Officer (OCIO) or DOT have developed and maintained an operational Business Continuity Plan and capabilities that would enable continued operation of critical business processes in the event of a disaster.

During our testing, we observed the following:

- Neither the OCIO nor DOT have a Business Continuity Plan or a formal Disaster Recovery Plan in place which should include defining recovery time objectives and maximum tolerable outage for DRIVES
- Critical business processes and their dependencies have not been identified
- DOT's evaluations of DRIVES criticality is incomplete, and the evaluation process did not follow a common methodology and deviated from industry guidance and standards

**Recommendation #6**

DOT, in collaboration/consultation with the OCIO, should:

- Conduct a formal Business Impact Assessment that identifies critical business processes, key people, processes and technology dependencies
- Define Recovery Time Objectives, Recovery Point Objectives and Maximum Allowable Downtime for the identified critical business processes and include third party vendors where necessary
- Following the completion of the Business Impact Assessment, leverage the targets and relevant information within the Business Impact Assessment to develop a Business Continuity Plan and a Disaster Recovery Plan, including any required IT resilience and recovery capabilities to meet Business Impact Assessment identified targets[10]
- Once complete, conduct a formal tabletop exercise to test and validate the Business Continuity Plan and conduct annual testing of plans to validate their function and identify gaps in execution

**Objective 7: Vendor Management and Controls – Gaps within contract terms and conditions with third party vendor identified**

Winding River Solutions Inc. (Winding River) is a key service delivery partner, responsible for the primary development of DRIVES and has been developing and maintaining DRIVES since its inception and launch in 2012. During our testing, we observed the following:

- GNWT does not have full and uninhibited access to the full suite of system documentation, as managed and produced by Winding River
- Contracts and service agreements do not have any transition clauses and expectations that account for instances where Winding River is unable to continue providing services
- Contracts and service agreements do not include any security or privacy expectations for Winding River to adhere to while providing services
- Contracts and service agreements do not outline, or set expected service levels and DOT does not conduct or request any scheduled reporting against service levels
- Contracts are only renewed on a 12-month cycle, as opposed to a period that more closely reflects planned development work and tasks.

**Recommendation #7**

We recommend that DOT include the following clauses within their contract/agreement with Winding River:

- Clauses or terms that ensure that GNWT and DOT have complete access to the full suite of system documentation, as managed and produced by Winding River during development activities

[10] DOT and GNWT are recommended to leverage the industry guidance within *COBIT 5 - Enabling Processes, Chapter 5, DSS04* "Manage Continuity" and; ISO 27001:2013

- Specific transition clauses and expectations that account for instances where Winding River is unable to continue providing services. Such clauses should force or pre-emptively enable the transfer of system development functions, system knowledge and solution documentation over to DOT or a newly selected third party provider
- Security and privacy expectations including how to manage and secure personal information encountered during their contracted activities. Security and privacy expectations may include expectations of security of data, security within their development, operational and hiring practices and privacy expectations around access to personal data, personal data storage and location provisions.

  Oversight clauses and measureable Service Level Agreements (SLAs) Operating Level Agreements (OLAs) with vendor performance/service level monitoring and reporting against the defined targets. SLAs and OLAs should ensure that appropriate services and performance metrics are established and that there are processes related to governance and reporting. DOT may wish to consider establishing key service delivery expectations leveraging industry standards and guidance such as COBIT or ITIL and evolve service delivery targets using maturity benchmarking methodologies
- DOT may also wish to consider extending the contract length with Winding River which would more closely align to planned DRIVES development activities and timelines (i.e. establishing a three (3) to five (5) year support arrangement with Winding River.)

# 2.0 DETAILED AUDIT REPORT

## 2.1 Introduction and Background:

In January 2016, the Government of the Northwest Territories (GNWT) engaged Grant Thornton (GT) to conduct an Operational Audit of the Deh Cho Bridge (Bridge) Toll Revenue process, performed by the Department of Transportation (the Department or DOT). As part of this audit, procedures were requested to be conducted on the Toll Revenue process. GNWT uses DRIVES as its motor vehicle information system and SAM is the financial system used by DOT.

The Northwest Territories Deh Cho Bridge Act (the Act) requires all registered owners of northbound commercial vehicles weighing over 4,500 kg to pay a toll to cross the Bridge. Private, service and commercial vehicles weighing less than 4,500 kg are exempt from paying the toll fees.

The gantry, located near the Bridge in Fort Providence, is equipped with an Electronic Toll Monitoring (ETM) system that consists of high-resolution cameras and sensors to collect vehicle information when vehicles pass the gantry. Vehicle information is transmitted to the Department's motor vehicle information system, DRIVES, located in Yellowknife. Employees in the Inuvik office review these events during standard GNWT working hours. The toll revenue for all Bridge crossings is reconciled by the Department's South Slave office in Hay River.

The Department began operating the Northwest Territories' (NWT) first toll Bridge on December 1, 2012. The number of commercial vehicles that crossed the Bridge and the toll revenue collected is listed in the table below (information in the table below was provided by DOT):

| Fiscal Year | # of Vehicles | Budget ($000) | Actual ($000) |
|---|---|---|---|
| 2012-2013 | 6,589 | 1,300 | 1,427 |
| 2013-2014 | 16,578 | 4,010 | 3,921 |
| 2014-2015 | 18,466 | 4,010 | 4,463 |

For the period of April 1, 2015 to January 31, 2016 the number of northbound commercial vehicles weighing over 4,500 kg that crossed the Bridge and the toll revenue collected is listed in the table below:

| Period | # of Vehicles (A)<br>(Per DRIVES raw data[11]) | Actual Revenue (B)<br>(Per DRIVES Toll Reconciliation[12]) | Average $ per crossing<br>(C = A / B) |
|---|---|---|---|
| April 1, 2015 to January 31, 2016 | 12,998 | $3,121,927 | $240 |

[11] DRIVES raw data – an extraction from DRIVES provided by the Manager, Information Systems
[12] DRIVES tolling reconciliation – a report GT extracted from DRIVES for all tolling events that generated revenue

**Focus of the Internal Audit:**

The objectives of the operational audit were to determine if:

1. **Governance Framework** - The Act, regulations, policies, procedures and other relevant frameworks were clear, understood, and current to allow DOT staff and management to collect all eligible Bridge toll revenue;
2. **Information integrity** - The Bridge toll revenue information was relevant, reliable, accurate, complete and timely to allow the Department's staff & management to collect and use the information to manage the revenue collection;
3. **Compliance** - The processing of Bridge toll revenue was in compliance with the Act, Regulations, Bridge Toll Remittance Agreement, Access to Information and the Protection of Privacy Act, Financial Administration Act, Financial Administration Manual and Visual Identity Program;
4. **Asset Safety** - The Bridge gantry and toll revenue was safe, secure, and fully accounted for;
5. **Efficiency and Effectiveness** - There were adequate controls in place to allow for the effective and efficient processing of Bridge toll revenue transactions;
6. **Business Continuity** - The business continuity plans and the related controls covering people, process, and technology are appropriate to support DRIVES over the next three (3) to five (5) years; and
7. **Vendor Management and Controls -** The vendor (Winding River Solutions Inc. (Winding River)) has an appropriate internal control capacity to support DRIVES over the next three (3) to five (5) years.

Our audit scope covered the period from April 1, 2015 to January 31, 2016. All transactions and operations related to the Bridge tolling during that time period were considered within the audit scope.

In order to obtain an understanding of risks and existing controls relevant to the tolling revenue process, the engagement team conducted a preliminary risk assessment. Through the conduct of the preliminary risk assessment, key risks were identified and linked to the applicable audit objective. Based on these risks, we developed audit criteria that were tested during the audit. Please see Appendix A for details on the Audit Criteria.

The audit team conducted site visits to – the Department (Yellowknife), Finance & Administration (Hay River), the Bridge gantry (Fort Providence) and Winding River (Alberta). We visited Winding River to perform interviews and assess their internal control capacity.

Findings are based on the evidence and analysis from both the initial risk assessment and the execution of our audit work program. Observations are presented below by Objective.

## 2.2 Observations:

### 2.2.1 Objective 1: Governance Framework

The following Acts and Regulations were reviewed as part of this audit:

- The Bridge Act
- Deh Cho Bridge Regulations
- The Financial Administration Act
- The Access to Information and Protection of Privacy Act
- The Deh Cho Bridge Toll Remittance Agreement
- The Financial Administration Manual (FAM)

- The Visual Identity Program

The audit found that the applicable Acts, Regulations and policies noted above were clear and understood by management and individuals responsible for activities throughout the process. Additionally, users and stakeholders have access to certain guidance documents through the help function tool located in the DRIVES System. The audit found the DRIVES Administrator Manual available through the help function.

Procedural documents are also in place that describe the tolling process in more detail. In February 2015, DOT began developing a Deh Cho Tolling Procedures Manual (Tolling Procedures Manual or Manual) which is a comprehensive guide of the tolling process. The Tolling Procedures Manual contains an overview of each role (by level and name), associated responsibilities, expected outcomes, screenshots and visual instructions. Through interviews conducted, the Manual appears to be well understood by users and stakeholders.

Although the Tolling Procedures Manual was developed, we found that certain processes were not included and for detailed procedures, the responsible individual was not always identified. For example, the Manual provides detailed procedures around how to identify duplicate events but there is no indication of the individual responsible. Furthermore, the Manual does not define and outline the following processes:

- Permit purchasing
- Semi-monthly reconciliation between DRIVES and the bank account
- Finance review of batch transactions
- Payment intake/processing, collections, account receivable

In addition, comments, mark-ups and questions were found in the Tolling Procedures Manual. This indicates that the final versions may not be available to the individuals responsible for the process steps.

At the time of the audit, the Tolling Procedures Manual was not available to the users and stakeholders through the help function. A draft version of the Tolling Procedures Manual was distributed by the Manager, Information Systems on December 8, 2015. The Manual included in the email contained comments, markups and questions indicating a final version may not be available.

### Recommendation #1

We recommend that DOT management:

- Finalize the Tolling Procedures Manual and include roles and responsibilities for each key processes and procedures (i.e. permit purchasing, semi-monthly reconciliation between DRIVES and the bank account, finance review of batch transactions, payment intake/processing, collections, accounts receivable processes, etc.)
- Update the help function to include the finalized Tolling Procedures Manual

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. Finalize Toll Manual and re-incorporate all processes including identifying roles and responsibilities in all key processes.<br>B. Update DRIVES help function to include the finalized toll manual. | A. May 2017<br>B. July 2017 |

### 2.2.2 Information Integrity

The Bridge tolling procedures were reviewed in order to establish whether toll revenue information was relevant, reliable, accurate, complete and timely to allow DOT staff & management to collect and use the information to manage the revenue collection. Specifically, relevant, reliable, accurate, complete and timely have been defined as the following:

- **Relevant**: information relates to the Bridge Tolling process
- **Reliable**: information can be trusted
- **Timely**: information is received at the most useful or opportune time
- **Accurate**: information is free from errors
- **Complete**: all important and relevant information is present

The audit assessed control design and effectiveness within the following key tolling processes:

- Purchase Permits
- Tolling Matchup/Escalation
- Tolling Event Review
- Tolling Remittance Reconciliation
- Vendor Accounts (SAM)
- Tolling Revenue Reconciliation
- Payment Intake, AR Monitoring and Collections

## A. Purchase Permits

Bridge users may purchase permits through a company called 24/7 Permitting Limited (24/7). 24/7 receives information from the carrier and will enter the information into DRIVES and a Moneris payment terminal[13]. In order to ensure that all revenue is collected and accounted for, semi-monthly reconciliations between DRVIES and SAM (bank account) are completed. As part of this audit, the audit team re-performed the reconciliation for certain months to assess whether the expected process and controls were being followed. It was expected that reconciliations were performed using the direct extracts from SAM and DRIVES, variances are tracked through SAM and that significant (greater than 1% of revenues) variances identified were explained.

The audit tests found that reconciliations were performed by the Finance group using direct extracts from SAM and DRIVES and the variances noted were not significant. Variances between the DRIVES reports and the bank account are accounted for using two methods: 1) manual adjustments 2) a general journal entry through SAM to an over/short account.

Variances unaccounted for through the manual adjustments are recorded to the over/short account. The balance of the over/short account for the period April 1, 2015 to January 31, 2016 was $11,652. Management indicated that the only items causing the variance are timing differences (purchases in one month recorded in DRIVES that have not been recorded in the bank). This account should balance to $0 automatically from month to month. It was found that this account is reviewed on a monthly basis.

## B. Toll Matchup / Escalation

Vehicles crossing the gantry activate sensors that are located in the road. Once the sensors are activated, the system will capture pictures of the vehicle, vehicle weight, transponder[14] information and speed. The DRIVES system automatically converts the following categories:

- **Automatic** - DRIVES uses the transponder information captured to match the vehicle to the carrier profile in DRIVES

[13] Moneris payment terminal – A debit/credit machine set up at 24/7 that links directly to the GNWT bank account
[14] Transponder – a device kept on the carrier's vehicle that transmits a signal to the gantry system. The signal will identify the transponder number.

- **Below Qualifying Weight** - the weight captured by the gantry system is below 4,500 kg and therefore no toll is required

If the automated match does not occur, the Enterprise Weigh Scale will attempt to convert the event to a converted status in one of the following categories:

- **Exempt** - The vehicle is deemed to be of a type that is exempt from needing a toll permit for the crossing (for instance service vehicles or GNWT registrations)
- **Manual** - matched manually to a permit or a carrier
- **Non-commercial** - The event was a non-commercial vehicle that would not require a toll permit
- **Images Unusable** - Image is not readable and cannot be used for matching
- **No Image** - No image is attached to the tolling event
- **Southbound** - Vehicle is traveling south and not subject to tolls
- **Duplicate** - The event is a duplicate of another event (examples include instances when a vehicle crosses between multiple lanes and triggers the sensors multiple times)

If an event cannot be matched to a carrier or moved to a conversion category above, it will be moved to Pending or Investigation.

- **Pending** - Event needs further investigation to be matched. Performed by either Finance team, Operations manager or Manager Transport Compliance Section
- **Investigation** - Operations Manager will research and investigate event

In the end, if the event cannot be charged to a carrier, it will be moved to No Match

- **No Match** - The event could not be matched to any record within the DRIVES system

During our audit period, there were 176,354 events per the DRIVES raw data[15]. The following is a distribution of events by category:

| Category | Number of events | % of events |
|---|---|---|
| **Automatic** | 7,160 | 4.06% |
| **Below Qualifying Weight** | 158,935 | 90.12% |
| **Exempt** | 1,293 | 0.73% |
| **Manual** | 5,838 | 3.31% |
| **Non-commercial** | 2,311 | 1.31% |
| **Images Unusable** | 50 | 0.03% |
| **No Image** | 8 | 0.01% |
| **Southbound** | 142 | 0.08% |
| **Duplicate** | 583 | 0.33% |
| **Pending** | 1 | 0.00% |
| **Investigation** | 0 | 0.00% |
| **No Match** | 33 | 0.02% |
| **Total** | **176,354** | **100.00%** |

[15] DRIVES raw data – an extraction from DRIVES provided by the Manager, Information Systems

We tested a random sample 159 events (0.09% of all events) from the categories noted above. We tested the events to assess:

- The accuracy of classification (e.g. that the event converted to the Exempt category was actually an exempt vehicle crossing)
- Whether issues with inactive transponders were noted and followed up on
- Whether all relevant information was accessible to test

The sample testing indicated the following exceptions:

- Four (4) of 159 events tested were classified in the wrong category and resulted in lost revenue with an approximate value of $960[16]. The four (4) errors noted were in either the Exempt or Duplicate categories. The details on the four (4) errors are as follows:
  - Exempt – The total population of Exempt events for the audit period was 1,293. Three (3) of the 30 or 10% of events tested in this category should not have been classified as Exempt. This represents potential lost revenues of $31,032[17]
  - Duplicate – The total population of Duplicate events for the audit period was 583. One (1) of the 15 or 7% of events tested in this category should not have been classified as Duplicate. This represents potential lost revenues of $9,328[18]
- Four (4) events did not include proper follow up on inactive transponders
- Five (5) events matched to a permit but did not show the permit information on the Toll Matchup screen

The audit also assessed information integrity on the entire population of events (176,354). The following observations were noted:

- 58 of 176,354 events were converted to a status of "No Image/Image Unusable". For these events either no pictures were captured by the system or the picture captured was not legible and therefore could not be used for matching. All of the 58 events were above the qualifying weight which may represent lost toll revenue of up to $13,920[19]
- 33 of 176,354 events were converted to a status of "No Match". For these events, DOT was unable to match an event to a carrier within DRIVES. All 33 events were above the qualifying weight, which may represent lost toll revenue of up to $7,920[20]. Furthermore there is no documentation in DRIVES indicating the rational for converting these events to "No Match" status

### Interface between the Electronic Toll Monitoring (ETM) system and DRIVES

Vehicles crossing the gantry activate sensors in the road. There are sensors at both ends of the gantry. Once the sensors are activated, the system will capture pictures of the vehicle, vehicle weight, transponder information and speed. Everything caught between the first sensor and the last sensor is defined as a loop, and each loop is defined as a vehicle record. The vehicle records are accumulated and retained at the gantry. At approximately 2am every day, the file is "scrubbed" to remove information from vehicles travelling in Lane 2 (traveling southbound, which do not require a toll to be paid). After the file is "scrubbed", the ETM system uses the File Transfer Protocol (FTP) to transfer the file into the DRIVES system.

[16] $960 = 4 events x $240 average price (average price per crossing per pg.6 of the report)
[17] $31,032 = 10% error rate x 1,293 events x $240 average price (average price per crossing per pg.6 of the report)
[18] $9,328 – 7% error rate x 583 events x $240 average price (average price per crossing per pg.6 of the report)
[19] $13,920 = 58 events x $240 average price (average price per crossing per pg.6 of the report)
[20] $7,920 = 33 events x $240 average price (average price per crossing per pg.6 of the report)

DOT Information Systems provided us with the FTP file and a DRIVES extract[21] for one (1) day during the audit period. We filtered the extract to remove the events that occurred in Lane 2 and then compared the number of records between the two (2) files. We found that the number of events in both the FTP file and the DRIVES file agreed with one another.

## C. Tolling Event Review

The Operations Manager, Transport Compliance Manager and Director of Road Licensing and Safety review and monitor Pending and Investigation categorized events. A review of manual matches is performed by the Hay River Finance group during the tolling reconciliation process to reassess the accuracy of the conversion. The Hay River Finance team will review the images associated with the event to ensure the proper carrier is being charged, constituting an effective process.

Although the Hay River Finance team indicated that reviews were occurring, there was no evidence of review for events that are moved to the following categories: Automatic, No Match, Exempt, Non-commercial, Image Unusable, No Image, Southbound and Duplicate.

## D. Tolling Remittance Reconciliation

On a monthly basis, the carrier submits a self-remittance ("Carrier Self-Remittance") indicating the number of crossings to DOT. This self-remittance is reconciled with the DRIVES Crossing Report to verify accuracy of the self-remittance. The reconciliations are perform on the 28th day of the following month or at the carriers' request. The two (2) reports are compared, differences are highlighted (i.e. carrier reports more crossing, carrier reports different class, carrier reports less crossings) and issues are resolved through follow up with the carriers.

Finance performs a match between the carrier report and the DRIVES report. If there is a variance between the carrier remittance and the events per DRIVES, the Hay River Finance team contacts the carrier and discusses the specific events that do not match. The Finance team will obtain concurrence from the carrier and bill the proper amount. This process helps ensure the completeness of the events billed to the carrier. If the carrier concurs that the events per DRIVES are correct, the Finance team invoices the amount recorded in DRIVES.

Our testing consisted of five (5) tolling reconciliations for the month of June 2015 and five (5) tolling reconciliations for the month of November 2015. We tested the following:

1) Whether the amount to be charged and agreed upon with the carrier was documented
2) Whether the amount per DRIVES agreed to the invoice/discrepancy letter
3) Whether the amount per the invoice/discrepancy letter agreed to the carrier account in SAM

There were no exceptions noted during testing.

## E. Vendor Accounts (SAM)

Once the carrier file is closed in DRIVES, the total event revenue, less any purchased permits, is sent to SAM to update the vendor account. The group of carrier files that is sent to SAM is called a batch. Finance reviews and approves DRIVES transactions before a batch is sent to SAM, and invoices are automatically generated and sent to the carrier.

The following observations were noted from DOT walkthroughs:

- There was a clear segregation of duties occurring: the Manager, Finance & Administration only has access to the SAM approve function and Finance staff only have access to the SAM-review function
- Manager, Finance & Administration reconciles the batch total from DRIVES to the batch total per the manual spreadsheet that Finance uses to track amounts charged to carriers

[21] DRIVES extract – All events for the day was provided by the Manager, Information Systems in excel format

## F. Deh Cho Bridge Toll Revenues Reconciliation

A monthly reconciliation is performed between revenue recorded in SAM and DRIVES. During this process, all variances above 1% of total revenues should be identified and explained.

During the audit, we requested the reconciliations for the months April 2015 to December 2015. We expected that all reconciliations for the period were completed and that all significant variances were explained. All of the reconciliations for the period were performed and the monthly variances and total variance were both under the 1% threshold. As a separate test, we re-preformed the reconciliations for the period of April 1, 2015 to December 31, 2015, using SAM and DRIVES extracts provided by the Finance manager. Our reconciliation resulted in a variance of 0.5% of total revenues for the period, which is not significant.

## G. Payment Intake, Accounts Receivable (AR) Monitoring and Collections

The payment intake, AR Monitoring and collections processes occur at the end of the tolling process, focusing on the collection of money.

The audit found appropriate segregation of duties throughout the payment intake process. The administrative assistant receives the mail and prepares a listing of cheques received. There is a second administrative assistant that will witness the opening of mail and the receipt of monies. The cheques are sent to an individual on the Finance team in charge of the carrier. This individual will enter the cheque into SAM and prepare a package of payments. This package is reviewed and signed off by the Finance Manager. The cheques are deposited into the account by the Finance team. On a monthly basis, the Finance Manager will perform a bank reconciliation.

FAM 3102 allocates the responsibilities for AR monitoring based on the number of days receivable. The Department's Finance group is responsible for monitoring and collection of receivables between 0 and 120 days. At 121 days, the receivable monitoring becomes the responsibility of the Department of Finance which is not part of the tolling process.

The balance of AR relating to tolling as at March 16, 2016 per the Aged AR listing[22] was $241,063, which represents 7.19% of tolling revenues for the audit period. The chart below outlines AR balances by days and AR as a percentage of revenues.

| AR Balances | | | | | | | |
|---|---|---|---|---|---|---|---|
| Age | Total | 0 – 30 days | 31 – 60 days | 61 – 90 days | 91 – 120 days | 120+ days | Bad Debt |
| AR | $241,063 | $125,918 | $98,153 | $2,068 | $11,394 | $1,328 | $2,202 |
| AR % of Revenues for the period | 7.19% | 3.75% | 2.93% | 0.06% | 0.34% | -0.04% | -0.07% |

During our walkthrough of the AR monitoring process, we expected that monitoring be performed on a timely basis (monthly) using an Aged AR report from SAM and that balances are followed up with carriers. Through our walkthrough the following was observed:

- There are no defined timelines for the review of AR balances and follow up with the carrier
- The Finance team does perform some follow ups with carriers but this is on a sporadic basis
- The Finance team uses Manual spreadsheets to track balances instead of an Aged AR report

We selected three (3) carriers with AR balances between 91 – 120 days to test whether follow ups were being performed on a timely basis. The results of our testing are as follows:

- For two (2) out of three (3) carriers tested, there was no supporting documentation on follow up with carrier[23]

[22] The Aged AR listing was extracted from SAM and filtered to only include AR relating to tolling
[23] See recommendation #3 for specific recommendations on accounts receivable monitoring

### Recommendation #2

We recommend the following:

- Implement a risk-based review process that enables the detection of events that have been misclassified to a category that does result in a toll revenue. Higher risk events could include conversions to Exempt, Non-commercial, Image Unusable, No Image, Southbound, Duplicate and No Match
- In collaboration with the third party vendor that supports the bridge technology, conduct a review of the events that were deemed "No Image / Image Unusable" and determine the root cause of the image deficiency. Following the review, implement actions to help reduce the risk of the image deficiencies

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. A new subscription report for Northbound Vehicles >4,500 that were not matched to revenue has been developed. This report includes events for the past seven days that were classified as "No Match", "Exempt", "Duplicate", "Images Unusable", "No Image", "Investigation", and "Pending". This will be available from the DRIVES report menu option, and will allow the user to select any date range. Upon final acceptance from the Toll Working Group, the report will be scheduled and emailed to the Registrar of Motor Vehicles with a CC to the Manager, Transport Compliance. This report will be reviewed and signed off by the Registrar and will be kept on file for proof of compliance to policy. The Registrar of Motor Vehicles will determine the interval in which this information will be reviewed and/or to address any findings.<br>B. Formalize a predetermined schedule to review tolling events with the vendor. Schedule quarterly reviews with IRD on Tolling deficiencies. | A. November 2016<br>B. December 2016 |

### 2.2.3 Compliance

As part of this audit, compliance with applicable Acts and Regulations were assessed, specifically focusing on:

- The Deh Cho Bridge Act
- The Deh Cho Bridge Regulations
- The Financial Administration Act
- The Access to Information and Protection of Privacy Act
- The Financial Administration Manual
- The Visual Identity Program

## A. Deh Cho Bridge Act

The Deh Cho Bridge Act prescribes the Government to charge a toll for use of the Bridge. The Deh Cho Bridge Act includes a requirement for the creation of a fiscal year report relating to information about vehicles that cross the Bridge (i.e. amount of tolls collected in relation to vehicle type, vehicle class or configuration), costs of administering the toll collection program and other information deemed relevant by the Minister[24].

Through discussion with management, this report was not prepared or submitted to the Registrar. Consequently, the DOT was not in compliance with this provision of the Deh Cho Bridge Act. Effective March 1, 2016 this provision was removed from the Deh Cho Bridge Act.

Section 9, within the Enforcement section of the Deh Cho Bridge Act, prescribes a fine not exceeding $5,000 when a person contravenes the Act[25]. For instance, fines should be issued when an individual crosses the Bridge without arranging to pay the applicable toll (pursuant to section 6 or the Act). During the audit testing period, it was found that 15 of the 33 events converted to No Match could be identified by a visible license plate[26]. These vehicles crossed the Bridge without paying the appropriate toll and it was found that no fines were issued in these instances.

## B. Deh Cho Bridge Regulations

Provisions of the Deh Cho Bridge Regulations assessed through this audit relate to required tolling, toll permit providers, transponder providers and remittance agreements.

The regulations require that an operator or registered owner of a commercial vehicle travelling northbound across the bridge pay a toll. Commercial vehicle means a motor vehicle used for business purposes that has a gross weight exceeding 4,500 kg. During the audit period, 158,935 of 176,354 events were converted to a status of "Below Qualifying Event Weight". It was found that 1,337 of the 158,935 events in this category were above 4,500 kg. The reason for this is that the DRIVES system is configured to allow for a 10% tolerance on vehicle weight. Therefore vehicles up to 4,950 kg would be automatically converted to a category that does not generate toll revenue. This is not in compliance with the regulation and may represent a potential for lost revenues of up to $320,880[27] if all events were for commercial vehicles.

The Deh Cho Bridge regulations require DOT to obtain specific information on each carrier. For permit providers, this includes a unique serial number; the date and time of issue; the date and time that it comes into effect; the date and time of expiry; the vehicle license plate number and jurisdiction; the vehicle identification number; the type, class or configuration of the commercial vehicle; the total amount charged; and any other information that the Registrar requires[28].

For transponder providers, this includes the invoice serial number; the date of issue of the invoice; the transponder identification number; the name and address of the transponder provider; the name and address of the registered owner of the vehicle for which the transponder is provided; the vehicle license plate number and jurisdiction; the vehicle identification number; the total amount charged; and any other information that the Registrar requires[29].

We tested four (4) single use permits and 10 transponder invoices to determine if the required information was provided. There were no exceptions noted during the testing.

Carriers may apply to be toll remitters instead of purchasing permits. In this arrangement, the carrier tracks their monthly Bridge crossings and make payments to the DOT for crossings during the period. A remittance agreement is signed by carriers who chose this method of payment. According to the Regulations, all remittance

[24] Deh Cho Bridge Act, Tolls: Section 7.1

[25] Deh Cho Bridge Act, Enforcement: Section 9

[26] The distribution of jurisdictions for the license plates that were identifiable include: three (3) Northwest Territories, three (3) Alberta, three (3) Quebec, two (2) Ontario, one (1) Saskatchewan, and three (3) out of Country. Twelve of the 15 vehicle are registered within Canada.

[27] $320,880 = 1,337 events x $240 average price (average price per crossing per pg.6 of the report)

[28] Deh Cho Bridge Regulation, Toll Permit Providers: Section 4.5

[29] Deh Cho Bridge Regulations, Transponder Providers: Section 5.3

agreements must expire within one (1) year[30]. We selected five (5) remitters based on the November 2015 tolling remittance reconciliation to determine whether agreements were in place and that they expired within a year.

Testing results indicated that:

- Out of the five (5) agreements requested, three (3) agreements were provided to us for testing and two (2) were not be provided
- Of the three (3) agreements received, the agreement expired on an annual basis, as required by the Regulation

## C. The Financial Administration Act

The provision of the Financial Administration Act assessed through this audit related to the deposit of public money.

The relevant Act provision requires that every public officer ensure that all public money is deposited into the GNWT bank account[31]. The DOT has procedures in SAM that detail the deposit of money, billing and the cash drawer processes. Consequently, the DOT is in compliance with this provision of the Act.

Our testing consisted of five (5) tolling reconciliations for the month of June 2015. We expected that the payments for the tolling remittance received were deposited into the GNWT bank account and that the deposit was made on a timely basis. We tested that the payment matches SAM, that the payment went through the GNWT bank and that the deposit date was within two (2) days of when it is recorded in SAM. No exceptions were noted during our testing.

## D. The Access to Information and Protection of Privacy Act

Provisions of the Access to Information and Protection of Privacy Act assessed through this audit relate to providing notice to individual and protection of personal information when information is being collected.

This provision requires that the Department provide carriers the following information:

- The purpose for collection of information
- The legal authority for the collection
- A contact person

Through our review of the tolling website and the remittance agreement template, we did not observe this information being formally disclosed to the carriers.

## E. The Financial Administration Manual

Provisions of the Financial Administration Manual assessed through this audit related to the credit granting and control and revenue agency contracts.

The Credit Granting and Control provision requires the Department to engage in the following activities:

- Maintain and monitor accurate credit records, including aged accounts receivable
- Determine whether receivables are being consistently received when due
- Take vigorous collection action on overdue receivables[32], notifying the debtor in writing that the receivable is overdue 30, 60, and 90 days after the initial invoice[33]

During our walkthrough of the AR monitoring process, we expected that monitoring be performed on a timely basis (monthly) using an Aged AR report from SAM and that balances are followed up with carriers. Through

[30] Deh Cho Bridge Regulations, Remittance Agreements: Section 6.5
[31] The Financial Administration Act, Deposit of Public Money: Section 14.1
[32] The Financial Administration Manual, Control & Collection of Accounts Receivable – Credit Granting and Control: Section 3101 – 4.5.1
[33] Financial Administration Manual, Departmental and Public Agency Responsibility for Collection of Receivables – Collection Procedure for Receivables: Section 3103 – 4.3

our walkthrough the following was observed:

- There are no defined timelines for the review of AR balances and follow up with the carrier
- The Finance team performs periodic follow-up with carriers
- The Finance team uses manual spreadsheets to track balances instead of an Aged AR report

We selected three (3) carriers with AR balances between 91 – 120 days to test whether follow ups were being performed on a timely basis. Specifically, we requested documentation (emails, documented calls, etc.) indicating that follow-up on aged receivables was conducted. The results of our testing are as follows:

- For two (2) out of three (3) carriers tested, there was no supporting documentation demonstrating follow-up with the carrier occurred

Our walkthrough and testing suggest that due to a lack of defined timelines for follow ups and use of Aged AR reports, receivables may not be being monitored appropriately.

The Revenue Agency Contracts provision requires that 24/7 remit monies collected on a daily basis[34]. Our testing confirms that this is occurring in accordance with the Financial Administration Manual.

### F. The Visual Identity Program

The Visual Identity Program outlines the requirements for visual elements of the GNWT brand, including a pictorial logo and optional wordmarks, corporate fonts, a colour palette and other graphic elements. As part of the audit, tests were conducted to determine compliance against the requirements of the visual elements of the GNWT. Compliance was assessed against a presentation and two (2) business cards. There were no exceptions noted.

### Recommendation #3

We recommend that DOT management:

- Enforce and issue fines for vehicles that cross the Bridge without paying the appropriate toll
- Review the existing DRIVES weight threshold and make required changes to ensure compliance with the regulations. In addition, implement an ongoing re-calibration of the scales to help ensure increased accuracy of weight measurement; DOT may wish to consider referencing relevant guidance published and set forth by Measurement Canada[35] in evaluating the configuration/recalibration of the weighing scale and practices in collecting revenue from weighing scales and stations
- Improve document management practices to help ensure remittance agreements with carriers are maintained and can be accessed in an efficient manner
- Formally disclose the required information to carriers regarding access to information and privacy
- Ensure that follow-up on receivables is conducted in accordance with Financial Administration Manual requirements and documentation is maintained around follow-up actions

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. RLS Compliance now has legislation in place to charge carriers for toll evasion; RLS sometimes faces the | A. September 2016 – HTOs are now issuing fines however occasionally encounter challenges serving out of territory carriers with the fines. |

[34] The Financial Administration Manual, Alternative Service Delivery – Revenue Agency Contracts: Section 3561 – 5.1
[35] https://www.ic.gc.ca/eic/site/mc-mc.nsf/eng/Home

| | |
|---|---|
| challenge of finding Service Providers to serve tickets to clients in other jurisdictions.<br>B. The Department has over 95% confidence it is collecting all revenues. The Department made a deliberate decision to not include vehicles that were up to 10% over the weight classification of 4,500kg. The increased costs to certify the scales, added resources to collect possible revenue would outweigh any economic benefits. Further, the Department of Justice advised there was little/no chance of a conviction for toll evasion for these vehicles. The WIM scales at the gantry are only used to see if a unit is greater than 4500kg. Measurement Canada procedures are currently used to calibrate our static scales including the self-weigh scale. The intent was for tolling charges to strictly apply to commercial vehicles not passenger vehicles which due to the conditions of the north where additional gas tanks and snow/ice conditions are a factor passenger trucks hit the weight threshold. For that reason consideration is being given to updating the regulations to include/replace the weight qualification specification with a definition that refers to commercial vehicle configurations that would specifically exclude passenger trucks.<br>C. The department will be moving towards a DIIMS environment to aid in the storage of documents. Current practices will be reviewed to ensure that all documents are easily accessible.<br>D. Currently, the access to information and privacy policies are posted on the DOT website. The department will examine other methods of communicating the policies and procedures. The Department will consult with DOJ on specific wording.<br>E. Corporate Services will compile a new process for documenting and following up on collections. This new process will comply with the Financial Administration Manual. | B. Complete<br>C. September 2017<br>D. March 2017<br>E. December 2016 |

### 2.2.4 Asset and Data Security

#### A. Access Control

DRIVES was developed in partnership with GNWT and Winding River to replace the DOT's previous Motor Vehicle Information System. It was developed with access controls to address the Department's business needs, operating as the cornerstone driver license and tolling solution for the DOT to support the management of business functions and service delivery. As such, DRIVES capabilities and functions are broad and powerful. DRIVES processes a vast number of sensitive transactions such as driver licencing, account remittance and accidents. Thus, ensuring that access control to the system and key functions is important to maintain the security and integrity of tolling remittance and other key DRIVES capabilities.

We expected that access controls for DRIVES are adequately managed, appropriate, and documented. Specifically, we expected that account management is performed in accordance with DRIVES policies/standards and follows best practices for account authorization. We also expected that user role assignment and access privileges are appropriate and established access privileges enforce segregation of duty and least privilege principals (i.e. that access is limited to the minimum level that will allow for normal functioning).

DRIVES includes dynamic and flexible access control capability that enables users to be assigned a variety of roles to carry out their function and meet the DOT business needs. Access is guided by DRIVES access policies and a comprehensive Administrator Manual. These policies include defined procedures on how to create, manage and revoke access on a user account.

Account creation is limited to 12 people with a specific administrative function in DRIVES. Furthermore, the DOT has DRIVES access authorization policies. These policies include the requirement for completion of three (3) access forms, including the RCMP Criminal Records check, DRIVES User update Request and DRIVES User Guidelines forms. Additionally, by requiring an employee's manager to sign access forms, these managers have a central role in account creation. Security roles are assigned to access roles spanning from issuers and examiners to financial and administrative functions.

While DOT has established a comprehensive administration manual and supporting access policies, we found that documented procedures and policies for identity and access management, including account creation, role assignment and related controls, are either absent or lacking appropriate rigor.

Specifically, we found that the account authorization process is flawed in that there is no control or current capability to validate the required supervisor approval for access, and the entire process occurs outside of DRIVES with no way to easily audit access approvals/authorization. Further, all hardcopy records of account request and creation approvals, including the three (3) required forms, were identified as lost, and embedded system controls designed to confirm that background checks were reviewed prior to granting access are either incomplete or inconsistently performed. Resultantly, we could not perform testing to validate that any user access was authorised as necessary documentation and data required for testing is missing.

Key account review findings include:

- Three (3) users were identified as having multiple accounts
- Several user accounts do not have full user details entered (i.e. emails, complete username)
- 143 (~50%) of accounts cannot be validated to have been approved (check box functionality not being used); there is no traceability of supervisor approval

Compounding account creation gaps, we found that the assignment of privileges to a user account was performed inadequately. DOT has not established a Role Based Access Control Matrix to guide or instruct the assignment of access privileges to identified resources or profiles within DOT. Role and privilege assignment is done based off the account manager/creator's interpreted understanding of the user's needs. Access request forms do not indicate the level of required access and without a Role Based Access Control Matrix, DRIVES account creators take a best effort approach to assigning access privileges. The audit found that a number of users have been assigned system-access privileges without an apparent, documented business need. Twenty-four unique users have privilege assignment that is not in line with expected separation of duties and least privilege principles. This allows some users to create, modify, and approve transactions, including financial submissions to SAM.

Key account privilege assignment observations include the following:

- 10 users where a system admin function is combined with a business function
- 23 users where an examiner and issuer function were combined
- One (1) user/system administrator was found with 50 privilege assignments including privileges where examiner/issuer/administrator and a finance functions were combined

As highlighted above, the audit did identify gaps in the assignment of access privileges which indicates that segregation of duty and least privilege principals have not been followed. However, the audit could not fully validate the severity and breadth of the issue as DOT has not documented a Role Based Access Control Matrix or formally considered incompatible role assignment combinations. Without these key documents in place prescribing role assignments, detailed testing to confirm the appropriate assignment of access privileges within DOT could not be performed.

Notwithstanding the gaps in account creation and role assignment, DOT does not perform any periodic review of accounts and access privileges or key transactions outside of daily and monthly reconciliation activities. Once a user account is created and access privileges are assigned, the account is not reviewed unless the employee requests additional access permissions or if the employee leaves or is terminated from their role. Additionally, there is no oversight/reporting on account activities or transactions for those users that have broad and powerful access privileges or the ability to create, modify and approve transactions in DRIVES.

Key account review observations include the following:

- 10 IT Support personnel from Winding River had DRIVES accounts (since removed)
- Two (2) accounts have been improperly terminated/disabled

Without effective and accurate access controls and privilege assignment for DRIVES, DOT and GNWT are at risk of security and privacy breaches and an increased likelihood of fraud within the DRIVES system and its related operational functions. Further, poor account management can increase the time and effort required to identify system issues and conduct ongoing auditing.

## B. Tolling and Data Security

The collection of tolling revenue is critically dependant on the effective and secure operation of tolling equipment and technology at the Bridge gantry. The Bridge gantry is equipped with a myriad of technology and equipment including cameras, transponder readers, lighting and in-road weight scale equipment that collectively identifies, measures, tracks and reports on the type, size, frequency and ownership of each vehicle that uses the bridge. We expected that the Bridge gantry tolling equipment and technology was secured and accounted for.

We conducted an onsite review of the completeness and security of the equipment and technology assets located at the Bridge. The review identified the following equipment and technology located at the station:

- 11 cameras used for both vehicle recognition and onsite security
- Six (6) infrared lights/illuminators and power supplies to support night time photography
- Two (2) transponders for the south and north lanes
- Two (2) remote antennas for wireless transmissions and communications
- Two (2) control boxes and power transformers for processing and communications

The main equipment is supported with an alternate power coupler that can have a remote generator connected to it to support all equipment during the event of a power failure.

While we found that gantry maintenance authorities were unable to provide a listing of installed equipment to confirm the completeness of the identified equipment, we also found that there were no overt signs of missing equipment. All equipment appeared to be located and positioned in a manner to support tolling collection.

We also found that all equipment as reviewed was secured with appropriate hardware or locking mechanisms or that it was positioned in an elevated location exceeding 10 feet from the ground and generally out of the reach of people.

### Recommendation #4

DOT should take steps to review, update and enhance their overall Identity and Access Management controls and process for DRIVES. This would include the following:

- Conduct a full account review of DRIVES, validating access requirements, role assignment and privileges, ensuring that all accounts have the necessary authorization forms complete and that accounts are approved by an authorised representative. This review should identify accounts that are no longer used or are required to support DRIVES maintenance and support, such as the Winding River accounts. This review should be performed on an annual basis and supported through updated policies on account review
- Define an access control matrix for DRIVES that outlines baseline role and privilege assignment, conflicting roles, and plain descriptions of roles to guide to assignment of roles and privileges to users and groups
- Enhance the user account access and authorisation process to ensure that all user access requests have traceability, are formally authorised by appropriate supervisors or managers and have completed all the necessary background checks. This process and model should ensure that access requests capture the necessary details and identity data of a user and authorizer, including:
  - Full name, email and contact details of requestor
  - Role and title of requestor
  - Requested level of access or system role (e.g. Examiner vs. Reviewer)
  - Full name, email and contact details of requestor manager/supervisor (with demonstrated authority and approval of access request)
  - Level of approved access or system role
  - Term of access required and approved
- DOT should identify and maintain a baseline listing of installed equipment at the gantry, including device details and model numbers

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. Conduct a user account review and update all relevant documentation and user accounts as required. *Formalize schedule to review users access on an annual cycle.*<br>B. Create an access control matrix. Review user account roles to ensure they have the appropriate level of access. This will be reviewed and signed off by the Registrar. | A. March 2017<br>B. March 2017<br>C. March 2017<br>D. June 2017 |

| | |
|---|---|
| C. The Manager of Driver and Vehicle Licensing Programs has full authority to grant access to the DRIVES system. Before granting access, a background check consisting of the following is completed:<br>• Full name, email and contact details of requestor<br>• Role and title of requestor<br>• Requested level of access or system role (e.g. Examiner vs. Reviewer)<br>• Full name, email and contact details of requestor manager/supervisor (with demonstrated authority and approval of access request)<br>• Level of approved access or system role<br>• Term of access required and approved.<br>From time to time, this authority will be delegated to respective users in their absence. The Manager of Driver and Vehicle Licensing Programs will keep a log of who was granted this delegation authority and provide the Registrar of Motor Vehicle with a copy of this approval. A monthly audit report listing all account modifications taking place during the month will be designed, generated, reviewed, signed off and filed by the Manager of Driver and Vehicle Licensing Programs. A copy of the report will be reviewed with the Registrar on a quarterly basis. Any account modifications made without the authorization of the Manager of Driver and Vehicle Licensing Programs and a complete background check will be reported to the Registrar Motor Vehicles within three business days for further investigation and further action taken as required. In consultation with the Registrar, the Manager of Driver and Vehicle Licensing Programs and the Registrar Motor Vehicles will determine the corrective actions that will take place once this investigation is complete.<br>D. Update catalogue of DCB Gantry onsite inventory. | |

### 2.2.5 Efficiency and Effectiveness

Please refer to section 2.2.2 of this report for the results of the audit procedures and testing related to process and control effectiveness. In the below section, observations and opportunities for improvement specifically focused on process and controls efficiencies are summarized.

Through the conduct of the audit, process and control documentation was reviewed and walkthroughs were performed to determine whether process and controls were designed and operating in an efficient manner. It was observed that various controls were automated resulting in improving efficiencies throughout the process. Specific efficiencies were found within the toll matchup process and included:

- Automated conversions: based on transponder information and the vehicles being under qualifying weight
- Valid permits appear on the side of the DRIVES Tolling Matchup screen so that they are easily identifiable
- There are search functions that the individual can use to find the carrier (e.g. unit number, plate number, transponder number, client name).

Although efficiencies were found throughout the process, opportunities were identified to further optimize the tolling process and controls. Specific examples include:

- Manual adjustments during the semi-monthly reconciliation may not be required given that all variances should be accounted for in the over/short account analysis that is performed at the end of the month
- Hay River Finance is tracking invoices and payments using a manual spreadsheet. Tracking and monitoring these amounts is a good practice, but this can be conducted through the SAM system. SAM can generate reports based on the information in the system, therefore these manual spreadsheets would not need to be used.
- There is no tracking mechanism to follow-up on issues related to matching. Currently the Finance Administrative Staff, Finance Manager, Operations manager, Transport Compliance Manager and the Director of Road Licensing and Safety all follow up on issues related to matching

### Recommendation #5

We recommend that DOT management:

- Explore the opportunity to remove manual adjustments to the semi-monthly reconciliation
- Enhance user awareness of the information, reports and functionality that can be generated from SAM with regards to accounts receivable management
- Implement a follow-up tracking mechanism for issues that arise from the automated matching process and identify specific individuals responsible for the follow-up procedures

### Management Response to Recommendation #5:

| Action Plan | Completion Date |
|---|---|
| A. Management previously reviewed and tried to implement the suggested option of removing manual adjustments without success. The number and amount of the manual adjustments are currently immaterial and management feels that given the current number of staff the costs would exceed the incremental benefits of this proposal.<br>B. A staff orientation will be provided to increase user awareness of the information, reports and functionality. | A. Complete<br>B. December 2016<br>C. March 2017 |

| | |
|---|---|
| Example of A/R reports and collections procedures will be added to the manual.<br><br>C. Implement issue tracking for toll matching process. There will be a quarterly review of the issue resolution logs that are being prepared by the Registrar. This will be tracked through the DCB Toll Working Group meeting minutes. An action tracking sheet will be developed to identify actions and persons responsible with timelines. | |

### 2.2.6 Business Continuity

Business Continuity capabilities and planning enable the secure and timely recovery of critical services for an organization or public entity and are considered a fundamental operational and strategic capability. Key GNWT and DOT practices and capabilities were reviewed to determine if the Office of the Chief Information Officer (OCIO) or DOT, has developed and maintained an operational Business Continuity Plan (BCP) and capabilities that would enable continued operation of critical business processes in the event of a disaster. Specifically, we expected that the OCIO, the Technology Service Centre (TSC) or DOT had conducted necessary business criticality and resumption planning activities that include developing a Business Impact Assessment (BIA), necessary Disaster Recovery Plans (DRP) and capabilities and BCPs and capabilities to support the continued delivery of critical services.

Specifically we assessed whether:

- DOT and/or the OCIO has operational or organizational BCPs and supporting documentation
- DOT and/or the OCIO has completed a BIA or equivalent that outlines or captures the recovery requirements of critical processes that support tolling revenue collection and processing
- TSC and/or DOT has completed IT DRPs and supporting documentation such as backup procedures and policies

We reviewed various internal service level agreements and practices and key documentation that supports or directs business continuity planning, including risk assessments and service continuity priority listings.

While neither the OCIO nor DOT have a BCP in place, we found that there are some organizational elements that would support the effective development and execution of a DRP. These include documented priorities, recovery time objectives and the maximum tolerable outage for key IT systems and sub systems including DRIVES. Additional information and context on system criticality that would feed the development of a BIA does also exist in the following documents:

- A Threat and Risk Assessment (TRA) completed in 2013
- An IT Risk Assessment completed in 2013

We found that Service Level Agreements for the TSC are in place and that these include core operational practices, such as maintaining network availability and backup and recovery services for key IT systems including DRIVES. A backup schedule is in place for DRIVES, and backup practices meet the defined schedule and include the backing up of key data and configurations of the system. The system backup schedule is automated and follows industry standards, with daily incremental and weekly full backups being performed. Backup logs are produced and emailed to key managers as evidence of successful backup. Additionally, backups leverage secure and mature technologies and are stored offsite in an effective and secure manner.

The entire DRIVES application is restored on a regular basis as part of testing and release practices. While this function is not performed as part of any specific recovery testing activities, it demonstrates that the application can be restored from backups and that staff is familiar with the process.

While TSC is currently developing a DRP, it is being developed without identifying critical business processes and conducting a BIA. Those elements, that are already defined and would support the effective development and execution of a DRP, have also been developed without identifying critical business processes as would be conducted during a BIA. Compounding this gap, the DRIVES system criticality, as evaluated in the 2013 TRA, differs from what has been set in the documented IT System priority schedule. The 2013 TRA evaluated the criticality of DRIVES as Low, and the documented IT System priority schedule set the criticality of DRIVES as High. Further, there is no formal or informal documentation or assessment that identifies or evaluates any recovery point objectives for DRIVES or critical processes.

Notably, neither the OCIO nor DOT have conducted a BIA, meaning that critical processes have not been identified and key people, processes and technology dependencies necessary to support those critical processes are unknown. As the DOT's documented priorities, recovery time objective and the maximum tolerable outage allowances for DRIVES are IT system centric and not business process centric, any newly developed Disaster Recovery capabilities, while improving IT resilience and redundancy, may still fall short of meeting business requirements. They may also erroneously invest in deploying unnecessary IT redundancy and resilience in areas that do not require it.

Without identifying critical processes and evaluating their dependencies and recovery targets, DOT and GNWT will not be able to develop an accurate DRP or a BCP that meets departmental or territorial needs. Furthermore, without these fundamental controls and capabilities in place, GNWT and DOT will not be able to effectively recover from any major disaster event in a manner that meets business or the public expectations, and DOT may not be able to provide critical services during a major event or disaster.

### Recommendation #6:

DOT, in collaboration/consultation with the OCIO, should:

- Conduct a formal BIA that identifies critical business processes, key people, processes and technology dependencies
- Define Recovery Time Objectives, Recovery Point Objectives and Maximum Allowable Downtime for the identified critical business processes and include third party vendors where necessary
- Following the completion of the BIA, leverage the targets and relevant information within the BIA to develop a DOT focused BCP and a DRP, including any required IT resilience and recovery capabilities to meet BIA targets[36]
- Once complete, conduct a formal tabletop exercise to test and validate the BCP and conduct annual testing of DRPs to validate their function and identify gaps in execution

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. Conduct a formal Business Impact Assessment. | A. June 2017<br>B. March 2017 |

[36] DOT and GNWT are recommended to leverage the industry guidance within *COBIT 5 - Enabling Processes, Chapter 5, DSS04* "Manage Continuity" and; ISO 27001:2013

| | |
|---|---|
| B. Develop and implement a formalized Recovery Plan.<br>C. Develop Business Continuity Plan and a Disaster Recovery Plan. Other departments that are completing this process are currently being consulted for best practices.<br>D. Conduct formal tabletop exercise. | C. March 2017<br>D. June 2017 |

### 2.2.7 Vendor Management and Controls

Winding River is a key service delivery partner, responsible for the primary development of DRIVES and has been developing and maintaining DRIVES since its inception and launch in 2012. Key GNWT and Winding River practices and controls were reviewed to determine if appropriate internal controls and capacity were in place to support DRIVES over the next three (3) to five (5) years. Specifically, it was expected that Winding River had effective and mature development practices in place that are appropriate for the development and maintenance of the DRIVES system, those processes are defined/documented and standards, procedures, and tools for software assurance are in place.

We expected that Winding River has a demonstrated history of service and client delivery and operational capacity to continue to deliver services for DOT and GNWT and to support DRIVES. We also expected that agreements between Winding River and GNWT included security and privacy provisions, service expectations and that reporting against expectations is conducted periodically.

Winding River was reviewed in four (4) core areas:

1. Development maturity and capability
2. Service delivery and continuity
3. Security and Privacy
4. Service Level Agreements and oversight

#### A. Development Maturity and Capability

Winding River development managers were interviewed to understand development practices, and onsite walkthroughs of development practices and procedures of Winding River were conducted. We also reviewed DRIVES system development documentation and outputs to determine their existence and completeness against expectations.

We found that Winding River produces various documents to support and guide their development efforts and projects for DRIVES. A review of sampled Business Requirements documents and Statements of Work/Proposals identified that Winding River clearly outlines the key elements and system details within their system development process and methodology.

Furthermore, Winding River leverages detailed test documents to guide the level of detail and completeness of testing activities. This includes stand-alone test documents and details on testing embedded within their development management tool. The development management tool is accessible to DOT and GNWT resources and has embedded mapping of development activities to key business and system requirements documentation stored on Winding River internal repositories.

We found that DRIVES is a continuously evolving system and system documentation is also an evolving component of its continued development. Stand-alone static documents that describe the system from end to end do not exist in a central document; key system details, including those found in the detailed Business Requirements Documents, do outline relevant system/application details. While DRIVES code repositories exist with both Winding River and DOT and many development artefacts are produced by Winding River., we found that DOT does not set out any prescriptive expectations for the delivery or review of development artefacts. Document and report style deliverables are defined and delivered by Winding River, and GNWT and DOT's staff review and approve them in a relatively unstructured and informal manner.

While DRIVES system development is effectively documented and key development artefacts are in place and current, DOT does not have full and uninhibited access to the full suite of system documentation, as managed and produced by Winding River and may not be able to transition or manage DRIVES if Winding River, at some point in the future, is no longer the development partner and service provider.

**B. Service Delivery and Continuity**

Key controls were reviewed to confirm that key provisions and coverage for operational resilience and recovery/resumption of services are in place and to validate that Winding River's current service delivery capacity can meet the DRIVES development and maintenance horizon, including any planned upgrades and improvements.

We found that Winding River is a small but reliable service provider, which has been in operations for over 10 years. Winding River is operated by three (3) principal owners with 11 core employees located both in Edmonton, Canada and Serbia. Winding River is also a Certified Microsoft Silver Partner, and it diversifies its service offerings to ensure a steady revenue stream. Winding River offers and delivers the following key services to its clients:

- Custom Software Solutions
- IT Consulting and Business Analysis
- Project Management
- Microsoft product optimization services
- Infrastructure/Networking Solutions
- Systems Integration
- Training & Mentoring

Winding River's major clients are primarily large organizations or provincial government entities similar to the DOT/GNWT. Winding River has served the following clients over the past five (5) years:

- The Canadian Patient Safety Institute
- Nine (9) Departments/Ministries within the Government of Alberta
- McGill University
- Suncor
- Transport Canada
- The University of Alberta

We found that Winding River's relationship with DOT and GNWT has existed since 2005, with contracts generally increasing in size and value over their 10 year relationship.

We noted that the three (3) year planning document between DOT and Winding River identifies target builds and updates to the DRIVES system on top of standard maintenance activities and tasks. The development horizon does not identify any large development projects that exceed Winding River's previous or current workloads, nor does it identify the need or use of new technologies, platforms or programing languages different from its current build. We found that Winding River's development and business analysis team composition includes development resources in both Canada and Serbia and that there are no gaps in Windings River's current capacity to deliver anticipated development workloads.

As outlined in the service agreement, Winding River is obligated to provide support to resolve second and third level issues that TSC and DOT staff are unable to resolve. Agreements outline some additional services indicating that Winding River will support DOT and TSC in the event of a significant outage, including assisting with backup and restore processes. They will also provide general technical and advisory support requested by the DOT on any matter pertaining to the installation, configuration and ongoing management of the software application, including tier three (3) level support of the DRIVES application.

At the time of the audit, Winding River was noted as having the resources and capacity in place for the planned three (3) year horizon of planned development work, a demonstrated history of service and client delivery for government clients and a long-standing successful service delivery relationship with DOT.

However, this audit did identify that the GNWT and DOT's dependence on Winding River to develop and support DRIVES has progressively increased over their 10 year relationship and that core business analysis and knowledge of DOT functions and processes resides with Winding River resources, not within GNWT or with DOT resources. While there is some redundancy and capability within DOT and GNWT, much of the intimate knowledge gained in mapping business processes and integrating them into DRIVES does not exist within GNWT. Furthermore, contract terms between Winding River and GNWT only exist for a maximum of 12 months with no long-term plan on ensuring that key knowledge within Winding River can be leveraged over a three (3) to five (5) year period or that that knowledge will be transferred to GNWT or DOT resources.

Winding River is obligated to provide support to resolve second and third level issues and provide additional services that can support GNWT in the event of a significant outage. However, agreements between Winding River and GNWT do not have any clauses and expectations that require Winding River to support GNWT to recover services and resume system operations in the event of a significant or undue outage. Nor are there any clauses and expectations that require Winding River to assist with service transition in the event that they are no longer selected or able to provide development and support services.

In addition, the service agreement with Winding River does not have any transition clauses and expectations that account for instances where Winding River is unable to continue providing services. Such clauses would force or pre-emptively enable the transfer of the system development functions, business knowledge and solution documentation to GNWT or a newly selected third party provider.

Without effectively establishing and managing vendor or in-house capacity to maintain and develop DRIVES, there is a risk that DRIVES may progressively evolve to not meet client needs or it may experience untimely outages and gaps in processing.

Further, an absence of transition clauses or transition planning may be a challenge for DOT and GNWT in smoothly transitioning development services to a new service provider in the event that Winding River can no longer provide services. Furthermore, DRIVES may experience periods of delayed updates and necessary changes to meet public and internal needs. DRIVES may go unsupported for an undue period of time.

### C. Security and Privacy

The Winding River and GNWT/DOT contract and related controls were reviewed to confirm that key security and privacy provisions were in place between the two (2) parties.

Contracts outline standard GNWT terms on satisfactory work, including adherence to relevant privacy legislation, project work plans and Statements of Work. These are developed and submitted by Winding River to GNWT/DOT for approval to outline some intended security related activities and practices.

While some general privacy and security statements are embedded in agreements, contracts as reviewed do not include any security or privacy expectations for Winding River to adhere to while providing services. Those statements that do exist in agreements and Statements of Work are not obligatory components for Winding River to win contracts or complete the work to a satisfactory standard.

Without detailing and setting security and privacy expectations for third party vendors, DOT may experience an unintentional security and privacy breach via services and systems maintained by third party vendors, such as Winding River. Furthermore, DOT and GNWT may be held accountable for such a breach, as expectations have not been clearly communicated to partners and third party vendors, including Winding River.

### D. Service Level Agreements and Oversight

Contracting and agreement controls between Winding River and GNWT were reviewed to determine if Service Level Agreement expectations, methods for measurement and reporting against expectations have been established. We also attempted to determine if reporting against expectations occurred in accordance with the contract.

Draft Statements of Work, as developed by Winding River, outline some terms and descriptions of agreed to support levels that will be provided by Winding River. These include terms, or commitments for Winding River to acknowledge and respond to any critical and non-critical problem within 24 hours of notification and resolve the problem as soon as possible (typically within 24 hours or one (1) week) depending on criticality. Additionally, there are terms that outline Winding River's commitment to investigate, analyse and support the resolution of reported issues within DRIVES, including backup and recovery, tier three (3) technical support and advisory support.

Furthermore, general terms in contracts indicate that all work must be completed to the satisfaction of GNWT; however, this is a standard clause with no specific or nuanced reference to DRIVES or Winding River tasks and deliverables.

There are no clauses, language or terms that clearly or firmly outline expected service levels. For those general terms of service that do exists, there are no firm service metrics and no expectation of clauses that direct reporting against each service expectation. Furthermore, there is no identified history of reporting or oversight against service delivery expectations, outside of GNWT's approval of key project artefacts and deliverables.

Winding River does not provide any frequent reporting on service levels in any manner. Furthermore, GNWT does not conduct or request any scheduled reporting against service levels. While some ad-hoc reporting on the current status of a development cycle does occur, all of the oversight filters through a single resource and is performed on an as needed/desired basis against unknown standards or performance.

Contracts, as reviewed, do not include any specific or implied expectation that GNWT will review or audit Winding River's work or that they expect any detailed or scheduled reporting on activities on service delivery. Service level targets or intentions, as defined by Winding River, are not binding, nor are they formally represented in contracts.

Without conducting formal service delivery oversight or having frequent reporting on service standards and deliverables in place for third party vendors, GNWT may not be able to demonstrate that procured services are delivered to an expected standard.

**Recommendation #7:**

We recommend that DOT include the following clauses within their contract/agreement with Winding River:

- Clauses or terms that ensure that GNWT and DOT have complete access to the full suite of system documentation, as managed and produced by Winding River during development activities
- Specific transition clauses and expectations that account for instances where Winding River is unable to continue providing services. Such clauses should force or pre-emptively enable the transfer of system development functions, system knowledge and solution documentation over to DOT or a newly selected third party provider

- Security and privacy expectations, including how to manage and secure personal information encountered during their contracted activities. Security and privacy expectations may include expectations of security of data, security within their development, operational and hiring practices and privacy expectations around access to personal data, personal data storage and location provisions. Oversight clauses and measureable Service Level Agreements (SLAs) Operating Level Agreements (OLAs) with vendor performance/service level monitoring and reporting against the defined targets should be included. SLAs and OLAs should ensure that appropriate services and performance metrics are established and that there are processes related to governance and reporting. DOT may wish to consider establishing key service delivery expectations leveraging industry standards and guidance such as COBIT or ITIL and evolve service delivery targets using maturity benchmarking methodologies
- DOT may also wish to consider extending the contract length with Winding River which would more closely align to planned DRIVES development activities and timelines (i.e. establishing a three (3) to five (5) year support arrangement with Winding River.)

### Management Response:

| Action Plan | Completion Date |
|---|---|
| A. DOT may consider adding clauses to future Winding River contracts granting GNWT and DOT complete access to the full suite of system documentation managed and produced by Winding River during development.<br>B. DOT may consider adding specific transition clauses and expectations that account for instances where Winding River is unable to continue providing services. Such clauses should force or pre-emptively enable the transfer of system development functions, system knowledge and solution documentation over to DOT or a newly selected third party provider.<br>C. DOT may consider security and privacy expectations including how to manage and secure personal information encountered during contracted activities. Security and privacy expectations may include expectations of security of data, security within development, operational and hiring practices, privacy expectations around access to personal data, personal data storage, and location provisions. Oversight clauses, measureable Service Level Agreements (SLAs), Operating Level Agreements (OLAs) with vendor performance/service level monitoring, and reporting against the defined targets may also be considered by DOT.. DOT may consider establishing key service delivery expectations leveraging industry standards and guidance such as COBIT or ITIL and evolve service | A. March 2017<br>B. March 2017<br>C. March 2017<br>D. March 2017 |

| | |
|---|---|
| delivery targets using maturity benchmarking methodologies.<br>D. DOT may consider extending the contract length with Winding River which would more closely align to planned DRIVES development activities and timelines (i.e. establishing a three (3) to five (5) year support arrangement with Winding River.) | |

## Appendix A – Audit Criteria

Based on the risk assessment completed, planning interviews and document review, the following audit criteria have been developed to support the audit objective.

| Objective | Audit Criteria |
|---|---|
| **1. The Act, Regulations, policies, procedures and other relevant frameworks were clear, understood, and current to allow DOT staff and management to collect all eligible Bridge toll revenue (Governance Framework)** | 1.1. Relevant Acts, Regulations, policies, and procedures are clear, understood, and are current<br>1.2. Relevant Acts, Regulations, policies, and procedures are available to all stakeholders<br>1.3. Procedural documents include detailed procedures by Level / stakeholder |
| **2. The Bridge toll revenue information was relevant, reliable, accurate, complete and timely to allow DOT staff & management to collect and use the information to manage the revenue collection (Information integrity)** | 2.1 18(a) |
| **3. The processing of Bridge toll revenue was in compliance with the Act, Regulations, Bridge Toll Remittance Agreement, Access to Information and the Protection of Privacy Act, Financial Administration Manual and Visual Identity Program (Compliance)** | 3.1 GNWT is compliant with the key regulatory and legislated requirements included in the Bridge Act, Deh Cho Bridge Regulations, The Financial Administration Act, The Access to Information and Protection of Privacy Act, The Deh Cho Bridge Toll Remittance Agreement, The Financial Administration Manual, The Visual Identity Program |
| **4. The Bridge gantry and toll revenue was safe, secure, and fully accounted for ( Asset Safety and Data Security )** | 4.1 18(a)<br>4.2 18(a) |
| **5. There were adequate controls in place to allow for the effective and efficient processing of Bridge toll revenue transactions (Efficiency and Effectiveness).** | 5.1 18(a) |
| **6. Business continuity plans and related controls covering people, process, technology are appropriate to support DRIVES over the next three to five years. (Business Continuity)** | 6.1 18(a)<br>6.2 18(a) |
| **7. The DRIVES solution support vendor (Winding River Solutions) has appropriate internal controls and capacity to support DRIVES over the next three to five years ( Vendor Management and Controls)** | 7.1 18(a)<br>7.2 18(a)<br>7.3 18(a) |

## APPENDIX B – FINDINGS RATING SCALE

Our findings are classified and prioritized according to the following risk-ranking methodology[37]:

| Risk Ranking | Description |
|---|---|
| 5. Extreme | ▪ Occurrence would have extreme impacts on stakeholders at the Government of Northwest Territories and,<br>▪ Existing controls are inadequate or non-existent, suggesting that this risk is almost certain to materialize |
| 4. High | ▪ Inability or significantly reduced ability to achieve expected results and organizational priorities, and<br>▪ Existing controls are very weak, suggesting that this risk is likely to materialize |
| 3. Moderate | ▪ Moderate impact on ability to achieve business objectives, and<br>▪ Existing controls are generally adequate (few significant weaknesses) suggesting that this risk is only moderately likely to materialize |
| 2. Minor | ▪ Limited impact on ability to achieve expected results and organizational priorities, and<br>▪ There are minor weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize |
| 1. Insignificant | ▪ There is little to no impact on the ability to achieve expected results and organizational priorities, and<br>▪ There are no significant weaknesses in the existing control environment, suggesting that this risk is unlikely to materialize |

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

Government of Northwest Territories
Gouvernement des Territoires du Nord-Ouest

MAY 30 2018

**CONFIDENTIAL**

File: 7820-20-GNWT-151-131

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

**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. Vince McCormick, Director, Corporate Services, INF

Government of Northwest Territories
Gouvernement des Territoires du Nord-Ouest

# INFRASTRUCTURE

## Access to Information and Protection of Privacy Assessment

Internal Audit Bureau

May 2018

Government of Northwest Territories Gouvernement des Territoires du Nord-Ouest

# INFRASTRUCTURE

## 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.*

Government of Gouvernement des
Northwest Territories Territoires du Nord-Ouest

**CONFIDENTIAL**

May 30, 2018

File: 7820-20-GNWT-151-131

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

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

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

## B. BACKGROUND

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

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

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 Infrastructure, 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 these privacy processes (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.
- Training the staff responsible for ATIPP compliance.
- Individuals providing personal information to Infrastructure be advised of their privacy rights.

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

## D. ACKNOWLEDGEMENT

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

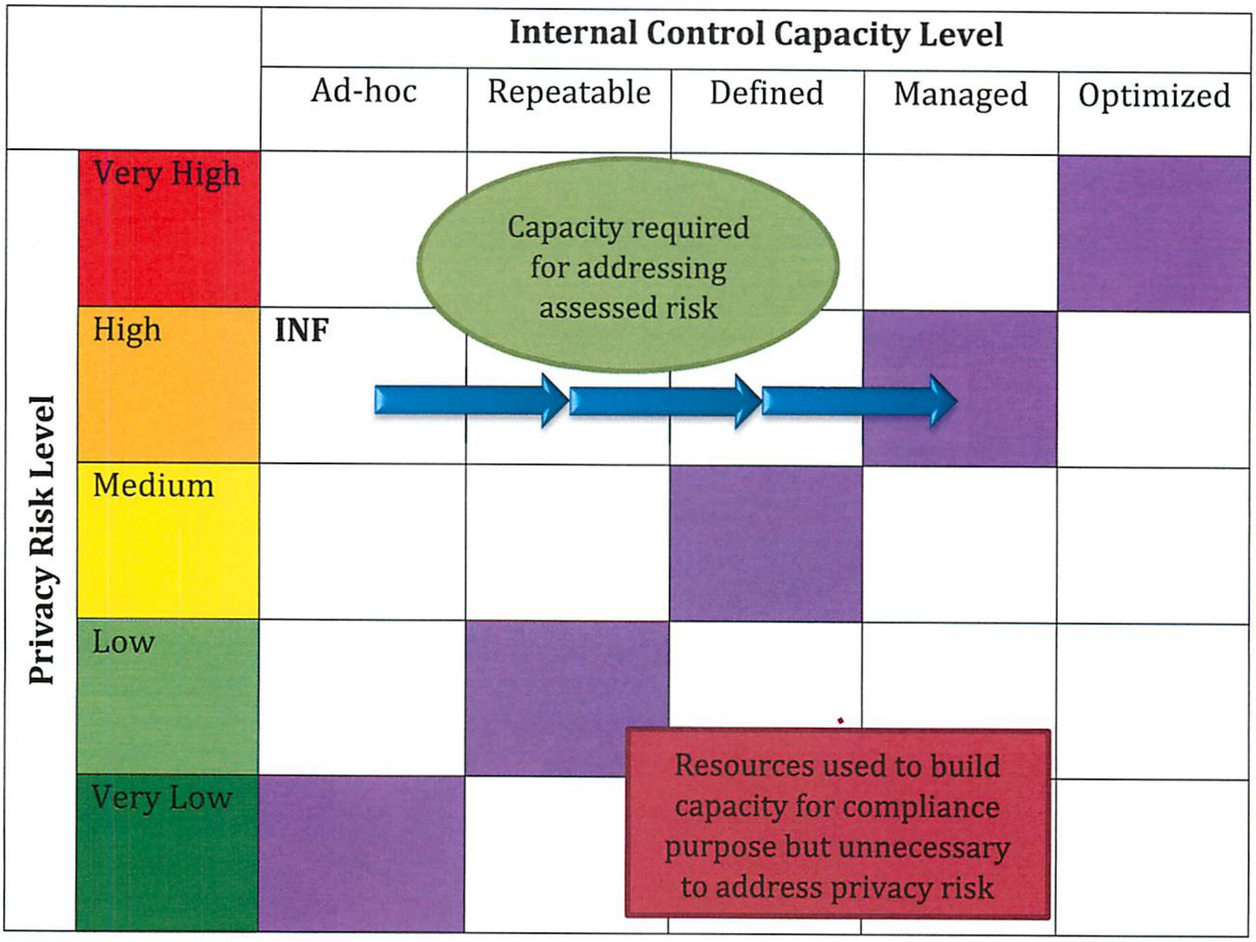
T. Bob Shahi
Director, Internal Audit Bureau
Finance

7820-20-GNWT-151-131
Access to Information and Protection of Privacy
As of March 31, 2018

**Chart I**

## Risk and Opportunity Assessment using Capacity Model

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



|  |  | Internal Control Capacity Level |  |  |  |  |
|---|---|---|---|---|---|---|
|  |  | Ad-hoc | Repeatable | Defined | Managed | Optimized |
| Privacy Risk Level | Very High |  |  |  |  | ■ |
|  | High | INF |  |  | ■ |  |
|  | Medium |  |  | ■ |  |  |
|  | Low |  | ■ |  |  |  |
|  | Very Low | ■ |  |  |  |  |

Capacity required for addressing assessed risk

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

Schedule I

# DEPARTMENT OF INFRASTRUCTURE

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

## Scope and Objectives

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

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

Infrastructure collects personal information through:

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

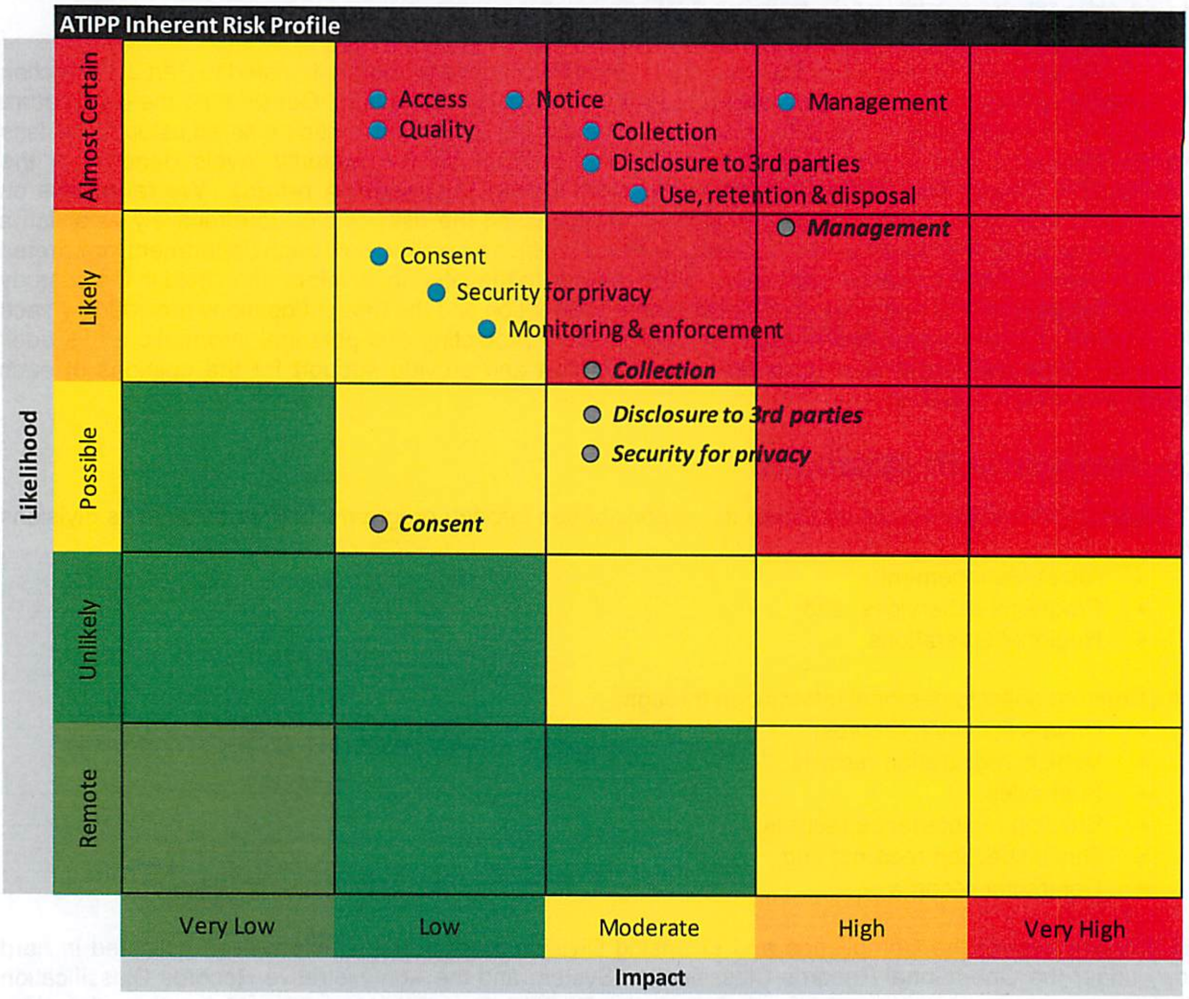
All divisions expect the Compliance and Licensing Division store personal information collected in hard copy under the Operational Records Classification System and the Administrative Records Classification System and electronic personal information on the Digital Integrated Information Management System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

## Overview

### Risk Profile

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

**RISK HEATMAP**



## Compliance with ATIPP Part 2 Protection of Privacy

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

# DEPARTMENT OF INFRASTRUCTURE

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

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

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

## Maturity Rating against Privacy Maturity Model

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

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

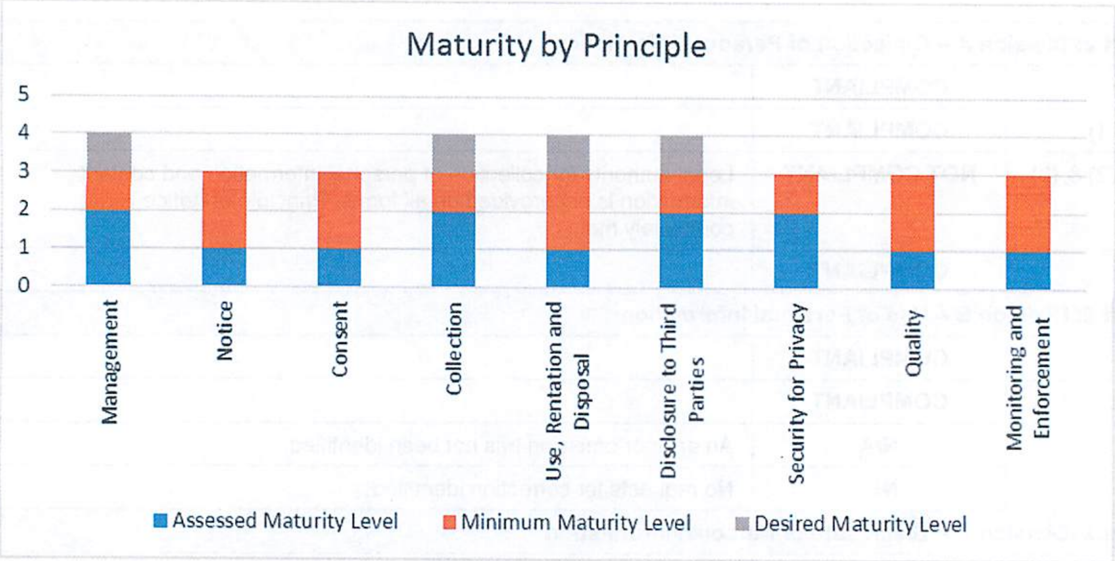
**Minimum Maturity Level** – In order to achieve this rating, the observations noted within this report must be addressed (short term timeframe 12-24 months).

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

# DEPARTMENT OF INFRASTRUCTURE

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

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



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

| Generally Accepted Privacy Principle | Assessed Maturity Level | Findings and Comments |
|---|---|---|
| **Management**<br>The department defines, documents, communicates and assigns accountability for its privacy policies and procedures. | Repeatable | • Privacy policies have not been formally designed and documented.<br>• An inventory does not exist of the types of personal information and the related processes, systems, and third parties involved.<br>• Procedures around the protection of privacy are largely undocumented<br>• An ATIPP Coordinator has been assigned and has taken the training offered by the Privacy Office.<br>• Privacy Risk Assessments are completed for all new processes and for old processes if an issue is brought forward.<br>• Training material with components of privacy has been developed for staff handling Compliance and Licensing personal information. |
| **Notice** | Ad Hoc | • A privacy policy has not been formally designed and documented to address notice to individuals. |

# DEPARTMENT OF INFRASTRUCTURE

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

| Generally Accepted Privacy Principle | Assessed Maturity Level | Findings and Comments |
|---|---|---|
| The department provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed. | | • Notice is not provided on all forms (hard copy and online) used to collect personal information.<br>*See observation 4.* |
| **Consent**<br>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. | Repeatable | • A privacy policy has not been formally designed and documented to address consent of individuals.<br>• Implicit consent is obtained on forms.<br>• Explicit consent is not obtained on all information forms.<br>*See observation 5.* |
| **Collection**<br>The department collects personal information only for the purposes identified in the notice. | Repeatable | • A privacy policy has not been formally designed and documented to address collection of personal information.<br>• The type of personal information collected and the method of collection for personal information collected by forms, in hard copy or online, is known to the individuals.<br>• Personal information from third parties is not accepted except from parties listed under the *Motor Vehicles Act* section 103 and 104 if a medical professional has grounds to believe the individual cannot operate a vehicle in a safe manner.<br>• Methods and forms of collecting personal information are not provided to the ATIPP Coordinator for review before implementation to ensure collection is fair and by lawful means.<br>• A documented procedure/process does not exist to ensure only personal information needed is collected.<br>*See observations 6-8.* |
| **Use, retention and disposal**<br>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. | Ad Hoc | • A privacy policy has not been formally designed and documented to address use, retention and disposal.<br>• A documented procedure/process does not exist to ensure personal information collected is only used for the purpose it was collected for.<br>• Retention and disposal of personal information is outlined in the Operational Records Classification System and the Administrative Records Classification System schedules and in the DIIMS which allows for personal information to be retained for no longer than necessary and is disposed of at that time, however not all documents have been moved over after the amalgamation of departments. |

## DEPARTMENT OF INFRASTRUCTURE

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

| Generally Accepted Privacy Principle | Assessed Maturity Level | Findings and Comments |
|---|---|---|
| | | • DRIVES is used to store all Compliance and Licensing personal information. DRIVES has no disposal dates programed, all historical data is being held indefinitely.<br>*See observation 7.* |
| **Disclosure to third parties**<br>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. | Repeatable | • A privacy policy has not been formally designed and documented to address disclosure to third parties and what remedial action should be taken if the personal information was misused by the third party.<br>• Information sharing agreements are in place with the exception of Statistics Canada. GNWT Legal Counsel was used in determining information sharing agreements were not necessary to provide personal information to Statistics Canada. |
| **Security for privacy**<br>The department protects personal information against unauthorized access (both physical and logical). | Repeatable | • 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.<br>• Logical access to personal information is restricted by the department through the use of DIIMS and DRIVES as well as database restrictions put in place.<br>• Security measures exist over the transmission of data but are not formally designed and documented.<br>• Database access audits are performed to determine if the correct individuals have access.<br>• Tests of safeguards in place are performed for the electronic environment.<br>*See observation 8.* |
| **Quality**<br>The department maintains accurate, complete and relevant personal information for the purposes identified in the notice. | Ad Hoc | • 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.<br>• There is no documented review process in place to ensure new forms developed by staff ensure personal information collected is relevant for the purpose identified.<br>*See observation 1 & 6* |

# DEPARTMENT OF INFRASTRUCTURE

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

| Generally Accepted Privacy Principle | Assessed Maturity Level | Findings and Comments |
|---|---|---|
| **Monitoring and enforcement**<br>The department monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes. | Ad Hoc | • A privacy policy has not been formally designed and documented to address monitoring and enforcement.<br>• Monitoring and enforcement are not being done at present although there have been reviews of controls in the past. Currently there are no scheduled or regular reviews<br>*See observation 1.* |

## Observations and Recommendations

### Observation 1

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

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

**Risk Profile:**

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

**Recommendations:**

We recommend that:

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

**Management Response:**

| Action Plan | Completion Date: |
|---|---|
| The Department of Infrastructure (INF) will work with the Department of Justice to ensure departmental processes and procedures are set up to allow INF to meet the requirements and guidelines of the Government of the Northwest Territories' (GNWT) privacy policy.<br>The Access to Information and Protection of Privacy (AT!PP) Coordinator and ATIPP staff will | INF will be fully compliant with the policy within one year of completion of the policy by the Department of Justice |

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

## Observation 2

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

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

### Risk Profile:

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

### Recommendations:

We recommend that:

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

### Management Response:

| Action Plan | Completion Date: |
|---|---|
| All INF divisions and regional offices will be asked to provide the INF ATIPP Coordinator with the following information:<br>• Every type of personal information collected by the division/office.<br>• The reason for the collection of each piece of personal information.<br>• The method in which that personal information is collected (divisions and regional offices will be expected to provide all physical forms, online form, etc.) | December 1, 2019 |

| | |
|---|---|
| • The staff positions who handle the information from collection to completion.<br>• The process for collection, storage, and deletion of the personal information.<br>• Systems used to collect/store the information.<br>• Third parties who have access to the information.<br>Once all of this information is collected from each division and regional office, the ATIPP Coordinator will combine the information into one global department inventory.<br>This information will be reviewed by the ATIPP staff to determine if the legislative authority exists for collection of the personal information, if unnecessary personal information is being collected, if the personal information is stored in a secure manner, to ensure only the necessary staff are handling the information, and to ensure the applicable privacy policies are followed. | |

### Observation 3

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

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

**Risk Profile:**

| | |
|---|---|
| Risk Impact | Without the proper training programs in place the ATIPP Coordinator cannot properly delegate work to ensue ATIPP compliance. |
| Risk Responsibility | Deputy Minister |
| Risk Mitigation Support | Delegated ATIPP Coordinator as well as the office of the GNWT Access and Privacy Office |

**Recommendations:**

We recommend that:

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

**Management Response:**

| Action Plan | Completion Date: |
|---|---|
| 23(2)(d) [redacted] has been asking for the appropriate ATIPP training from the GNWT Access and Privacy Office since INF was formed on April 1, 2017.<br>23(2)(d) [redacted] has completed the online ATIPP training but requires more in depth training to have a better understanding of the appropriate ATIPP processes and will take the | As soon as the ATIPP training is made available by the Access and Privacy Office. |

| | |
|---|---|
| training whenever it is offered by the Access and Privacy Office.<br>All INF staff who deal with personal information will be provided with a link to the online GNWT ATIPP training so they can complete the training and have a basic understanding of the ATIPPA. | |

## Observation 4

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

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

### Risk Profile:

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

### Recommendations:

We recommend that:

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

### Management Response:

| Action Plan | Completion Date: |
|---|---|
| As indicated under the action plan for Audit Report recommendation number two, the ATIPP Coordinator will ask all INF Senior Managers to provide all forms from their divisions or regional offices on which personal information is collected.<br>Once these forms are compiled the ATIPP staff will review the personal information being collected to determine if it is necessary and that the appropriate legislative authority exists to collect the information. Once this is completed, each form will be updated to comply with ATIPPA notice requirements, and will include:<br>• The purpose for which the information is collected<br>• The specific legal authority for the collection | December 1, 2019 |

| | |
|---|---|
| The title, business address, and business telephone number of an INF staff member who can answer questions about the collection. | |

## Observation 5

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

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

**Risk Profile:**

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

**Recommendations:**

We recommend that:

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

**Management Response:**

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

## Observation 6

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

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

**Risk Profile:**

| | |
|---|---|
| Risk Impact | Without a review of collection methods being introduced, there is increased risk of non-compliance with ATIPP legislation during these new collection methods. |
| Risk Responsibility | Director |

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

**Recommendations:**

We recommend that:

- A procedure be formalized that requires all new methods of personal information collection be reviewed and approved by the ATIPP Coordinator.
- A procedure be formalized that specifies that during their review the ATIPP Coordinator ensures only personal information needed for its use are being collected and it is being collected fairly and lawfully.
- A privacy impact assessment should be performed for all significant new personal information collection methods or changes to existing methods.

**Management Response:**

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

## Observation 7

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

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

**Risk Profile:**

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

**Recommendations:**

We recommend that:

- The department documents a process to reevaluate and reassess the current personal information collection needs to support the department mandate.

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

**Management Response:**

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

## Observation 8

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

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

**Risk Profile:**

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

**Recommendations:**

We recommend that:

- A review of records from pre-amalgamation be performed, and any sensitive personal information not related to the Compliance and Licensing Division, be moved from any identified older insecure systems to DIIMS. If personal information is held in a separate database that is up to date and secure, these items would be left as-is.

- A policy is implemented that outlines the scheduled disposal dates of all documents that are stored in the DRIVES system.
- The DRIVES system is updated to dispose of documents in accordance with ATIPP on the scheduled disposal date, or if it not possible to set up electronically, a manual system be implemented to delete these files.

**Management Response:**

| Action Plan | Completion Date: |
|---|---|
| All INF divisions and regional offices will be asked to review their records to determine if there is sensitive personal information being stored on older systems that may not be secure.<br>All divisions and regional offices, with the assistance of INF Information Technology staff, will need to determine if the databases have controls over who can access documents, if regular maintenance updates are completed, and if security measures are in place to keep the systems physically safe.<br>The network drives are physically secure and do undergo regular maintenance, and it is possible to restrict access to the folders beyond basic divisional and departmental settings. The Technology Service Centre will be asked to assist with further lockdowns if necessary. If sensitive personal information is found to exist on a system that is not secure, it will be moved into DIIMS.<br>In regards to the DRIVES system, records kept in this system are required to be maintained for longer periods of time when compared to other INF records. Retention of these records for longer periods is required to properly administer driver and vehicle related programs and the Motor Vehicles Act.<br>The Compliance and Licensing Division will develop a process that will require the Division to meet annually to determine if there are areas in DRIVES in which significant amounts of information/records are being maintained when there is no longer a purpose for them under the Motor Vehicles Act and associated regulations/programs. The process will also outline how such records would then be deleted. | December 1, 2019 |

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

**Appendix A**

# AICPA/CICA
# Privacy Maturity Model

March 2011

AICPA®

CA Chartered Accountants of Canada

# 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.

# AICPA/CICA Privacy Task Force

***Chair***
Everett C. Johnson, CPA

***Vice Chair***
Kenneth D. Askelson, CPA, CITP, CIA

Eric Federing

Philip M. Juravel, CPA, CITP

Sagi Leizerov, Ph.D., CIPP

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

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

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

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

***Staff Contacts:***
Nicholas F. Cheung, CA, CIPP/C
CICA
Principal, Guidance and Support

and

Nancy A. Cohen, CPA, CITP, CIPP
AICPA
Senior Technical Manager, Specialized Communities and Practice Management

**Acknowledgements**

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

ISACA®

Trust in, and value from, information systems

# Table of Contents

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 Model[1] 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.

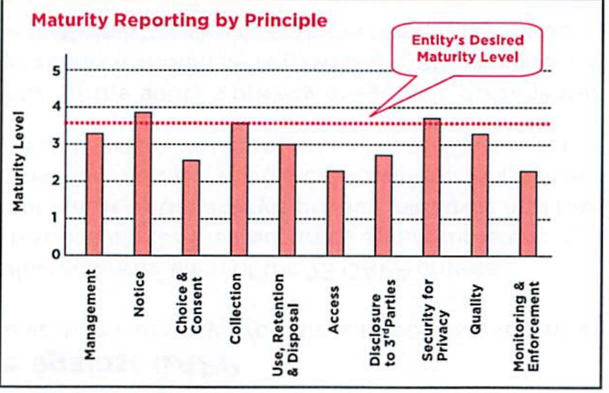
The following examples based on internal reports intended for management use graphical representations.

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

Figure 1 shows a sample graph that could be used to illustrate the maturity of the organization's privacy program by each of the 10 principles in GAPP.

The report also indicates the desired maturity level for the enterprise.

Reports like this are useful in providing management with an overview of the entity's privacy program and initiatives.



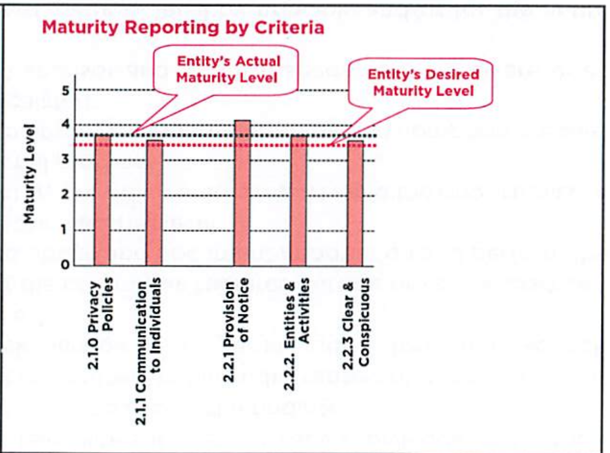
### Figure 2 – Maturity Report by Criteria within a Specific GAPP Principle

Figure 2 shows the maturity of each criterion within a specific principle – in this case, the 'Notice' principle.

The report indicates the actual maturity level for each criterion.

The report also indicates the actual and desired maturity level for the principle as a whole.

Reports like this provide useful insight into specific criteria within a privacy principle.

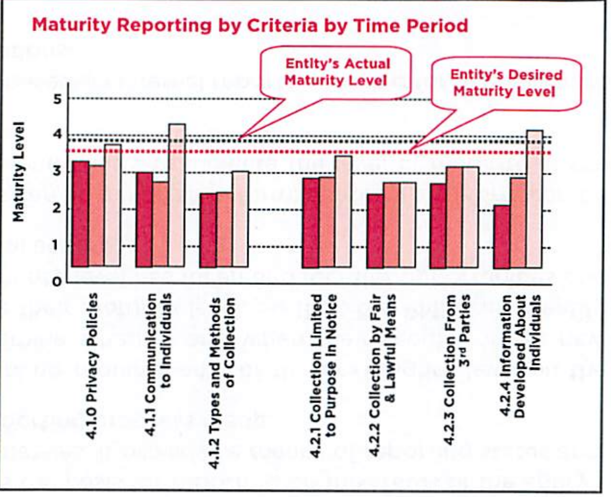


### Figure 3 – Maturity Report by Criteria within a GAPP Principle Over Time

Figure 3 shows the maturity of each criterion within the 'Collection' principle for three time periods.

The report indicates the actual maturity level for each criterion for three different time periods.

Reports like this provide useful insight into progress being made by the entity's privacy initiatives over time.



## 6 SUMMARY

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

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

# AICPA/CICA PRIVACY MATURITY MODEL[1]
# 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.**<br>**Changes in privacy policies are communicated to such personnel shortly after the changes are approved.** | Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented. | Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete. | The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program. | Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed. | Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved. |

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

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

| GAPP - 73<br>CRITERIA | CRITERIA<br>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.<br>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.**<br>**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 | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | 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.<br>Personal information is not adequately addressed in the entity's privacy and related security policies and procedures.<br>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.<br>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.<br>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.<br>For risk assessment, organizations may wish to use the AICPA/CICA Privacy Risk Assessment Tool. | Privacy risks are reviewed annually both internally and externally.<br>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.<br>Changes in the entity's privacy policies will trigger a review of existing contracts for compliance. | Contracts are reviewed on a regular basis and tracked. An automated process has been set up to flag which contracts require immediate review when changes to privacy policies and procedures are implemented. |

| GAPP - 73 | CRITERIA | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | 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)** | **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:**<br>**• Infrastructure**<br>**• Systems**<br>**• Applications**<br>**• Web sites**<br>**• Procedures**<br>**• Products and services**<br>**• Data bases and information repositories**<br>**• Mobile computing and other similar electronic devices**<br>**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.** | 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)** | **A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following:**<br>**• Procedures for the identification, management and resolution of privacy incidents and breaches**<br>**• Defined responsibilities**<br>**• A process to identify incident severity and determine required actions and escalation procedures**<br>**• A process for complying with breach laws and regulations, including stakeholder breach notification, if required**<br>**• An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate**<br>**• A process for periodic review (at least annually) of actual incidents to identify necessary program updates based on the following:**<br>**— Incident patterns and root cause**<br>**— Changes in the internal control environment or external requirements (regulation or legislation)**<br>**• Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed** | Few procedures exist to identify and manage privacy incidents; however, they are not documented and are applied inconsistently. | Procedures have been developed on how to deal with a privacy incident; however, they are not comprehensive and/or inadequate employee training has increased the likelihood of unstructured and inconsistent responses. | A documented breach management plan has been implemented that includes: accountability, identification, risk assessment, response, containment, communications (including possible notification to affected individuals and appropriate authorities, if required or deemed necessary), remediation (including post-breach analysis of the breach response) and resumption. | A walkthrough of the breach management plan is performed periodically and updates to the program are made as needed. | The internal and external privacy environments are monitored for issues affecting breach risk and breach response, evaluated and improvements are made. Management assessments are provided after any privacy breach and analyzed; changes and improvements are made. |

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **MANAGEMENT (14 criteria) cont.** | **The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.** | | | | | |
| **Supporting Resources (1.2.8)** | **Resources are provided by the entity to implement and support its privacy policies.** | Resources are only allocated on an "as needed" basis to address privacy issues as they arise. | Privacy procedures exist; however, they have been "developed" within small units or groups without support from privacy specialists. | Individuals with responsibility and/or accountability for privacy are empowered with appropriate authority and resources. Such resources are made available throughout the entity. | Management ensures that adequately qualified privacy resources are identified and made available throughout the entity to support its various privacy initiatives. | Management annually reviews its privacy program and seeks ways to improve the program's performance, including assessing the adequacy, availability and performance of resources. |
| **Qualifications of Internal Personnel (1.2.9)** | **The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received the necessary training.** | The entity has not formally established qualifications for personnel who collect, use, disclose or otherwise handle personal information. | The entity has some established qualifications for personnel who collect, disclose, use or otherwise handle personal information, but are not fully documented.<br>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)** | **For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:**<br>**— Legal and regulatory**<br>**— Contracts, including service-level agreements**<br>**— Industry requirements**<br>**— Business operations and processes**<br>**— People, roles, and responsibilities**<br>**— Technology**<br>**Privacy policies and procedures are updated to reflect changes in requirements.** | Changes in business and regulatory environments are addressed sporadically in any privacy initiatives the entity may contemplate. Any privacy-related issues or concerns that are identified only occur in an informal manner. | The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented. | The entity has implemented policies and procedures designed to monitor and act upon changes in the business and/or regulatory environment. The procedures are inclusive and employees receive training in their use as part of an enterprise-wide privacy program. | The entity has established a process to monitor the privacy environment and identify items that may impact its privacy program. Changes are considered in terms of the entity's legal, contracting, business, human resources and technology. | The entity has established a process to continually monitor and update any privacy obligations that may arise from changes to legislation, regulations, industry-specific requirements and business practices. |
| **NOTICE (5 criteria)** | **The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.** | | | | | |
| **Privacy Policies (2.1.0)** | **The entity's privacy policies address providing notice to individuals.** | Notice policies and procedures exist informally. | Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented. | Notice provisions in privacy policies cover all relevant aspects and are fully documented. | Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages. | Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance. |
| **Communication to Individuals (2.1.1)** | **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.**<br>**If personal information is collected from sources other than the individual, such sources are described in the notice.** | Notice to individuals is not provided in a consistent manner and may not include all aspects of privacy, such as purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement. | Notice is provided to individuals regarding some of the following privacy policies at or before the time of collection: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement. | Notice is provided to individuals regarding all of the following privacy policies at or before collection and is documented: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement. | Privacy policies describe the consequences, if any, of not providing the requested information and indicate that certain information may be developed about individuals, such as buying patterns, or collected from other sources. | Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. |

| GAPP - 73 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.<br>Notice is provided using various techniques to meet the communications technologies of their constituents (e.g. social media, mobile communications, etc). |
| **Entities and Activities Covered (2.2.2)** | **An objective description of the entities and activities covered by privacy policies is included in the privacy notice.** | The privacy notice may not include all relevant entities and activities. | The privacy notice describes some of the particular entities, business segments, locations, and types of information covered. | The privacy notice objectively describes and encompasses all relevant entities, business segments, locations, and types of information covered. | The entity performs a periodic review to ensure the entities and activities covered by privacy policies are updated and accurate. | Management follows a formal documented process to consider and take appropriate action as necessary to update privacy policies and the privacy notice prior to any change in the entity's business structure and activities. |
| **Clear and Conspicuous (2.2.3)** | **The privacy notice is conspicuous and uses clear language.** | Privacy policies are informal, not documented and may be phrased differently when orally communicated. | The privacy notice may be informally provided but is not easily understood, nor is it easy to see or easily available at points of data collection. If a formal privacy notice exists, it may not be clear and conspicuous. | The privacy notice is in plain and simple language, appropriately labeled, easy to see, and not in small print. Privacy notices provided electronically are easy to access and navigate. | Similar formats are used for different and relevant subsidiaries or segments of an entity to avoid confusion and allow consumers to identify any differences. Notice formats are periodically reviewed for clarity and consistency. | Feedback about improvements to the readability and content of the privacy policies are analyzed and incorporated into future versions of the privacy notice. |

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

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

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

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **COLLECTION (7 criteria) cont.** | **The entity collects personal information only for the purposes identified in the notice.** | | | | | |
| **Types of Personal Information Collected and Methods of Collection (4.1.2)** | **The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice.** | Individuals may be informed about the types of personal information collected and the methods of collection; however, communications are informal, may not be complete and may not fully describe the methods of collection. | The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are neither fully documented nor fully described in the privacy notice. | The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are fully documented and fully described in the privacy notice.<br>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:<br>• be fully documented;<br>• distinguish the personal information essential for the purposes identified in the notice;<br>• 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. |

| 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.<br>Retention periods are not uniformly communicated. | Individuals are consistently and uniformly informed about use, retention and disposal of personal information.<br>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 | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | 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.<br>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.<br>Any discrepancies found are remediated in a timely fashion. |
| **ACCESS (8 criteria)** | **The entity provides individuals with access to their personal information for review and update.** | | | | | |
| **Privacy Policies (6.1.0)** | **The entity's privacy policies address providing individuals with access to their personal information.** | Informal access policies and procedures exist. | Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented. | Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented. | Compliance with access provisions in privacy policies and procedures is monitored. | Management monitors compliance with privacy policies and procedures relating to access. Issues of non-compliance are identified and remedial action taken to ensure compliance. |

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **ACCESS (8 criteria) cont.** | **The entity provides individuals with access to their personal information for review and update.** | | | | | |
| **Communication to Individuals (6.1.1)** | **Individuals are informed about how they may obtain access to their personal information to review, update and correct that information.** | Individuals may be informed about how they may obtain access to their personal information; however, communications are inconsistent, sporadic and undocumented. | Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated. | Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated. | Processes are in place to update communications to individuals when changes occur to access policies, procedures and practices. | The entity ensures that individuals are informed about their personal information access rights, including update and correction options, through channels such as direct communication programs, notification on statements and other mailings and training and awareness programs for staff.<br>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 be documented and may not be consistently applied. | Some procedures are in place to allow individuals to access their personal information, but they may not cover all aspects and may not be fully documented. | Procedures to search for an individual's personal information and to grant individuals access to their information have been documented, implemented and cover all relevant aspects. Employees have been trained in how to respond to these requests, including recording such requests. | Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided.<br>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 | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **ACCESS (8 criteria) cont.** | **The entity provides individuals with access to their personal information for review and update.** | | | | | |
| **Confirmation of an Individual's Identity (6.2.2)** | **The identity of individuals who request access to their personal information is authenticated before they are given access to that information.** | Procedures to authenticate individuals requesting access to their information are informal, not documented and may not be consistently applied. | Procedures are in place to confirm the identity of individuals requesting access to their personal information before they are granted access, but do not cover all aspects and may not be documented. Level of authentication required may not be appropriate to the personal information being accessed. | Confirmation/authentication methods have been implemented to uniformly and consistently confirm the identity of individuals requesting access to their personal information, including the training of employees. | Procedures are in place to track and monitor the confirmation/authentication of individuals before they are granted access to personal information, and to review the validity of granting access to such personal information. | The successful confirmation/authentication of individuals before they are granted access to personal information is monitored and periodically assessed for type 1 (where errors are not caught) and type 2 (where an error has been incorrectly identified) errors. Remediation plans to lower the error rates are formulated and implemented. |
| **Understandable Personal Information, Time Frame, and Cost (6.2.3)** | **Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.** | The entity has some informal procedures designed to provide information to individuals in an understandable form. Timeframes and costs charged may be inconsistent and unreasonable. | Procedures are in place requiring that personal information be provided to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost, but may not be fully documented or cover all aspects. | Procedures have been implemented that consistently and uniformly provide personal information to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost. | Procedures are in place to track and monitor the response time in providing personal information, the associated costs incurred by the entity and any charges to the individual making the request. Periodic assessments of the understandability of the format for information provided to individuals are conducted. | Reports of response times in providing personal information are monitored and assessed. The associated costs incurred by the entity and any charges to the individual making the request are periodically assessed. Periodic assessments of the understandability of the format for information provided to individuals are conducted. Remediation plans are made and implemented for unacceptable response time, excessive or inconsistent charges and difficult-to-read personal information report formats. Conversion of personal information to an understandable form is automated where possible and appropriate. |

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

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

| GAPP - 73 CRITERIA | CRITERIA DESCRIPTION | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| | | AD HOC | REPEATABLE | DEFINED | MANAGED | OPTIMIZED |
| **DISCLOSURE TO THIRD PARTIES (7 criteria) cont.** | **The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.** | | | | | |
| **Communication to Third Parties (7.1.2)** | **Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.** | Procedures to communicate to third parties their responsibilities with respect to personal information provided to them are informal, inconsistent and incomplete. | Procedures are in place to communicate to third parties the entity's privacy policies or other specific instructions or requirements for handling personal information, but they are inconsistently applied and not fully documented. | Documented policies and procedures exist and are consistently and uniformly applied to communicate to third parties the privacy policies or other specific instructions or requirements for handling personal information. Written agreements with third parties are in place confirming their adherence to the entity's privacy policies and procedures. | A review is periodically performed to ensure third parties have received the entity's privacy policies, instructions and other requirements relating to personal information that has been disclosed.<br>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.<br>Collection of consent for new purposes and uses is automated where possible and appropriate. |

| GAPP - 73 | CRITERIA | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | 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.<br>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)** | **A security program has been developed, documented, approved, and implemented that includes administrative, technical and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The security program should address, but not be limited to, the following areas[3] insofar as they relate to the security of personal information:**<br>**a. Risk assessment and treatment [1.2.4]**<br>**b. Security policy [8.1.0]**<br>**c. Organization of information security [sections 1, 7, and 10]**<br>**d. Asset management [section 1]**<br>**e. Human resources security [section 1]**<br>**f. Physical and environmental security [8.2.3 and 8.2.4]**<br>**g. Communications and operations management [sections 1, 7, and 10]**<br>**h. Access control [sections 1, 8.2, and 10]**<br>**i. Information systems acquisition, development, and maintenance [1.2.6]**<br>**j. Information security incident management [1.2.7]**<br>**k. Business continuity management [section 8.2]**<br>**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.<br>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)** | **Logical access to personal information is restricted by procedures that address the following matters:**<br>**a. Authorizing and registering internal personnel and individuals**<br>**b. Identifying and authenticating internal personnel and individuals**<br>**c. Making changes and updating access profiles**<br>**d. Granting privileges and permissions for access to IT infrastructure components and personal information**<br>**e. Preventing individuals from accessing anything other than their own personal or sensitive information**<br>**f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities**<br>**g. Distributing output only to authorized internal personnel**<br>**h. Restricting logical access to offline storage, backup data, systems and media**<br>**i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)**<br>**j. Preventing the introduction of viruses, malicious code, and unauthorized software** | Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete. | The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information. | The entity has documented and implemented security policies and procedures that sufficiently control access to personal information.<br>Access to personal information is restricted to employees with a need for such access. | 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.<br>Irregular access of authorized personnel is also monitored. | 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.<br>Irregular access of authorized personnel is monitored, assessed and investigated where necessary. |

| GAPP - 73 | CRITERIA | MATURITY LEVELS | | | | |
|---|---|---|---|---|---|---|
| CRITERIA | DESCRIPTION | 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.<br>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.<br>The entity may lack a business continuity plan that would require an assessment of threats and vulnerabilities and appropriate protection of personal information. | The entity has a business continuity plan addressing certain aspects of the business. Such a plan may not specifically address personal information. Accordingly, personal information may not be appropriately protected. Business continuity plans are not well documented and have not been tested. | The entity has implemented a formal business-continuity and disaster-recovery plan that address all aspects of the business and identified critical and essential resources, including personal information in all forms and media, and provides for specifics thereof. Protection includes protection against accidental, unauthorized or inappropriate access or disclosure of personal information. The plan has been tested. | Management monitors threats and vulnerabilities as part of a business risk management program and, where appropriate, includes personal information as a specific category. | Management risk and vulnerability assessments with respect to personal information result in improvements to the protection of such information. |
| **Transmitted Personal Information (8.2.5)** | **Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry-standard encryption technology for transferring and receiving personal information.** | The protection of personal information when being transmitted or sent to another party is informal, incomplete and inconsistently applied. Security restrictions may not be applied when using different types of media to transmit personal information. | Policies and procedures exist for the protection of information during transmittal but are not fully documented; however, they may not specifically address personal information or types of media. | Documented procedures that cover all relevant aspects have been implemented and are working effectively to protect personal information when transmitted. | The entity's policies and procedures for the transmission of personal information are monitored to ensure that they meet minimum industry security standards and the entity is in compliance with such standards and their own policies and procedures. Issues of non-compliance are dealt with. | Management reviews advances in security technology and techniques and updates their security policies and procedures and supporting technologies to afford the entity the most effective protection of personal information while it is being transmitted, regardless of the media used. |

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

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

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

| GAPP - 73 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. |

## NOTES

# Appendix A

AICPA®

CA Chartered Accountants of Canada

Government of Northwest Territories | Gouvernement des Territoires du Nord-Ouest

FEB 2 6 2018

**CONFIDENTIAL**

File: 7820-20-INF-151-100

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

**Infrastructure Airports Division - Safety Management System Triennial Audit**

Enclosed is the above referenced Audit Report.

We look forward to working with your staff on the next triennial audit. Please advise us by December 2019 should you wish to have this project included in the 2020-2021 Audit Work Plan for Audit Committee review.

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

T. Bob Shahi
Director, Internal Audit Bureau
Finance

Enclosure

c. Mr. Jamie Koe, Chair, Audit Committee
Ms. Delia Chesworth, Director Air Marine & Safety Division, Infrastructure
Mr. Vince McCormick, Director Corporate Services, Infrastructure

Government of Northwest Territories
Gouvernement des Territoires du Nord-Ouest

# INFRASTRUCTURE

## Airport Division
## Safety Management System Triennial Audit

Internal Audit Bureau - Operational Audit Report
February 2018

Government of Northwest Territories
Gouvernement des Territoires du Nord-Ouest

# Audit Report
## Operational Audit

## INFRASTRUCTURE
## Airport Division
## Safety Management System Triennial Audit

**February 2018**

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

Government of Northwest Territories    Gouvernement des Territoires du Nord-Ouest

**CONFIDENTIAL**

February 26, 2018

File: 7820-20-INF-151-100

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

**Infrastructure Airports Division - Safety Management System Triennial Audit**

At the request of the Department of Infrastructure, (Department), the Audit Committee authorized the Internal Audit Bureau (IAB) to provide independent assurance regarding the Department's compliance with the *Canadian Aviation Regulations (CARs) under the 1985 Transport Canada Aeronautics Act* (Act). The purpose of the audit was to assess the Department's policies and procedures for compliance with CARs Part 1 Subpart 7 Safety Management Systems (SMS) requirements. This audit was as of October 31, 2017. The previous independent audit was carried out by IAB as of August 31, 2014.

## A. BACKGROUND

On January 1, 2008, the Act formally instituted the requirement for a SMS for all certified airports. CARs Part 1 Sub Part 7 Section 107.02 required all certified airports to maintain a SMS to monitor compliance with CARs. Section 107.03 detailed nine areas that shall make up the SMS **(Appendix A refers)**. The SMS program was administered by the Department's Air Marine & Safety Division (Division). Based on guidelines provided by Transport Canada, the Division developed a SMS manual that was used to monitor compliance with CARs.

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

The SMS manual categorized the nine areas detailed by CARs to make up the SMS into six components as follows:

1. Safety Management Plan
2. Documentation
3. Safety Oversight
4. Training
5. Quality Assurance
6. Emergency Preparedness

The Department relied on the Quality Assurance (QA) program to monitor compliance with CARs and assess the overall effectiveness of the SMS program. QA Operational Audits were conducted once every three years by the Division staff that were operationally independent and impartial of the area being audited to monitor compliance with CARs. This audit focused on establishing whether the SMS program was in compliance with CARs.

The GNWT operated 27 airports of which 20 airports were certified by Transport Canada. The GNWT classified six airports as "A" and fourteen airports as "B" **(Appendix B refers)**. Seven airports were not required to be certified due to absence of scheduled traffic.

## B. INDEPENDENT AUDIT SYNOPSIS

The GNWT operated airports in the NWT in accordance with CARs as of October 31, 2017.

The key internal control to ensure Department's compliance to CARs was the "Quality Assurance" program (component 5 of SMS Manual) carried out by the Division staff. Our primary focus was the assessment of this key internal control. Based on the Department's concerns, feedback from Transport Canada and our risk assessment, we also assessed component 4 (Training) of the SMS manual for compliance with CARs.

We observed and interviewed Department staff during a walkthrough of the QA process in 3 "A" airports and 3 "B" airports to understand the processes and the Department staff's understanding of SMS requirements, guidance and direction provided for Corrective Action Plans (CAPS) and incident/event reporting process **(Schedule I refers)**.

We have all the detailed documents to support our assessment. We would have no issue sharing these detailed documents with Transport Canada or your staff.

We look forward to working with your staff on the next triennial audit. Please advise us by December 2019 should you wish to have this project included in the 2020-2021 Audit Work Plan for Audit Committee review.

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

T. Bob Shahi
Director, Internal Audit Bureau, Finance

Schedule I

## 2018-INF- Airport Safety Management System
## Infrastructure
## File No. 7820-20-INF-151-100
## As at October 31, 2017

### Quality Assurance Process Review by Internal Audit Bureau

| Airport | Date of visit/Interview | Procedure |
|---|---|---|
|  |  | 18(a) [redacted] |
| Norman Wells | October 26, 2017 | [redacted] |
| Deline | October 25, 2017 | [redacted] |
| Tulita | October 25, 2017 | [redacted] |
| Fort Simpson | November 16-17, 2017 | [redacted] |
| Yellowknife | December 5, 2017 | [redacted] |
| Lutselk'e | December 6, 2017 | [redacted] |

Notes:

| | |
|---|---|
| √ | = Procedure performed |
| NA | = Procedure not applicable |

Appendix B

## 2018-INF- Airport Safety Management System
## Infrastructure
## File No. 7820-20-INF-151-100
## As at October 31, 2017

## NWT Airports
## NWT Airports as of October 31, 2017

| Certified Airports | | | | Registered | |
|---|---|---|---|---|---|
| **"A" Airports** | **Region** | **"B" Airports** | **Region** | **Registered** | **Region** |
| Inuvik | Inuvik | Aklavik | Inuvik | Fort Liard | Deh Cho |
| Norman Wells | Sahtu Region | Fort McPherson | Inuvik | Jean Marie River | Deh Cho |
| Fort Simpson | Deh Cho | Paulatuk | Inuvik | Nahanni Butte | Deh Cho |
| Yellowknife | North Slave | Sachs Harbour | Inuvik | Trout Lake | Deh Cho |
| Fort Smith | South Slave | Tuktoyaktuk | Inuvik | Wrigley | South Slave |
| Hay River | South Slave | Ulukhaktok | Inuvik | Fort Providence | South Slave |
| | | Colville Lake | Sahtu | Fort Resolution | South Slave |
| | | Deline | Sahtu | | |
| | | Fort Good Hope | Sahtu | | |
| | | Tulita | Sahtu | | |
| | | Gameti | North Slave | | |
| | | Lutselk'e | North Slave | | |
| | | Wekweeti | North Slave | | |
| | | Whati | North Slave | | |
| **6** | | **14** | | **7** | |
| **Total number of Airports** | | | | **27** | |

**Certified Airports**

A= Have paved runways and managed by GNWT staff.

B= Have Gravel runways and managed by contractors usually municipal Governments.

**Registered** = Airports with no scheduled traffic are not required by Transport Canada to have a Safety Management System.

Appendix A

# 2018-INF- Airport Safety Management System
# Infrastructure
# File No. 7820-20-INF-151-100
# As at October 31, 2017

## Safety Management System Requirements
## Canadian Aviation Regulation (CARs) Part 1 Sub part 7 Section 107.03

| Item | Description |
|---|---|
| a) | A safety policy on which the system is based. |
| b) | A process for setting goals for improvement of aviation safety and for measuring those goals. |
| c) | A process for identifying hazards to aviation safety and for evaluating and managing the associated risks. |
| d) | A process for ensuring that personnel are trained and competent to perform their duties. |
| e) | A process for the internal reporting and analyzing of hazards, incidents and accidents and for taking corrective actions to prevent their recurrence. |
| f) | A document containing all safety management system processes and a process for making personnel aware of their responsibilities with respect to them. |
| g) | A quality assurance program. |
| h) | A process for conducting periodic reviews or audits of the safety management system and reviews or audits, for cause, of the safety management system; an |
| i) | Any additional requirements for the safety management system that are prescribed under these Regulations. |

Government of Northwest Territories    Gouvernement des Territoires du Nord-Ouest

FEB 14 2020

**CONFIDENTIAL** File: 7820-30-GNWT-151-113

DR. JOE DRAGON
DEPUTY MINISTER
INFRASTRUCTURE

**Audit Report: ICT Data Demographics**
**Audit Period: As of March 31, 2019**

## A. SCOPE AND OBJECTIVES

The Audit Committee approved the assessment of demographic data retained in Government of the Northwest Territories (GNWT) departments 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 in support of fiscal responsibility, accountability, and transparency.

This report identified issues specific to the Department of Infrastructure (Infrastructure). Some ICT issues beyond the control of Infrastructure 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 such as name, address, date of birth and Social Insurance Number.

The GNWT Informatics Policy Council's Information Management Policy (Policy) provides guidance for 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, provides guidance to departments on policy implementation.

Infrastructure had thirteen databases that contained demographic information. Out of the thirteen databases, DRIVES contained demographic information of over 80,000 clients and supported the delivery of five programs and services.

## C. OVERVIEW

The mobility of people and products in the NWT was dependent on the information contained in DRIVES. The integrity of DRIVES information supported the issuing of authentic, official documents to eligible applicants. as well as enforcing compliance with applicable rules and regulations.

We conducted data analysis on over 80,000 clients and made two observations **(Schedule I refers)**:

i. Data Accuracy: a small amount of inconsistent client data was identified in some fields such as height, age, and name.

ii. Data Completeness: for a number of records, data fields such as date of birth, weight, or height were not completed.

The details of the two observations were reviewed with operating management. Management agreed with the risk rating of high for both observations. Management took proactive action to correct the inconsistent data and will implement quality assurance/quality control internal controls to avoid future errors.

## D. ACKNOWLEDGEMENT

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

T. Bob Shahi
Director, Internal Audit Bureau
Finance

SCHEDULE I

# Department of Infrastructure
# ICT Data Demographics
# 7820-30-GNWT-151-113

## Observation 1: 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*
- Be sure to review the information with the client to ensure accuracy – *DRIVES Administrator's Manual, p. 73*

### Condition / Evidence

We conducted data analysis to validate the accuracy of unique client identifiers within the DRIVES demographic data by reviewing three DRIVES data tables: Name, Client, and Address.

1. The DRIVES **Name data table** contained about 172,900 records of individuals and organizations. Of those, 80,879 records were "Active." We identified the following exceptions:

| Category | Total |
|---|---|
| Given Name Symbol (- ' * , .) | 25 |
| Surname Symbol (- * , .) | 3 |
| Space before the name (Given, Surname, or Company name) | 8 |
| Name contains "&" or "/" | 4 |

2. We reviewed the DRIVES **Client data table** containing 80,869 records of individuals and organizations. Of those records, 52,786 were "Active" or "Pending." Review of the client database highlighted the following concerns:
   - 9 records indicate the client has an active record over 100 years of age.
   - 39 records indicate the client's weight as under 35 kg or over 250 kg
   - 74 records indicate the client's height as under 100 cm or over 210 cm
   - 62 records with eye and hair colour unknown

3. We also reviewed the DRIVES **Address data table**, containing 366,977 records and found six exceptions:
   - Two records with invalid Address Type ID
   - Four records with invalid/blank "IsActive" classification

4. An analysis was conducted within the **Name data table** to identify duplicate records. The following concerns were identified:
   - 451 active records with the same company name and different Client ID #
   - 22 active records with duplicate Client ID #s and unique client names
   - 865 active records that contain the same Surname, Given Name, and Date of Birth with different Client ID #s

| Risk/Consequence: | |
|---|---|
| • DRIVES program may not have up-to-date client information, which may impact eligibility to access services and/or permits.<br>• Demographic data shared across federal/provincial/territorial (FPT) programs may be inaccurate, effecting client's access to services.<br>• Inaccurate demographic data shared across FPT programs may negatively affect the government's reputation. | **Risk Rating:** High<br>**Likelihood:** Almost Certain<br>**Impact:** Moderate<br>**Risk Owner:** Director, Compliance & Licensing<br>Support:<br>• Director, Corporate Services, INF<br>• Manager, Driver & Vehicle Licensing Programs |

**Recommendations:**

1. Send out written instructions for:
   a. Persons with single names to use "-" in place of the first name.
   b. Duplicate files

2. Complete review of characteristic data during Quality Assurance/Quality Control (QA/QC).

3. Create and/or update policies and processes for:
   a. Single Name entries
   b. Quality Assurance/Quality Control (QA/QC) Process

| Management Response: | Timeline: |
|---|---|
| 1. Current files have been reviewed and fixed by amending, deactivating, or noting files for reparation at next issue. Written instructions have been communicated to issuers. | Complete |
| 2. Review of characteristic data completed to ensure accuracy. | Complete |
| 3. Management will create update policies to cover items related to single name entries and to the QA/QC process. | February 29, 2020 |

## Observation 2: Data 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)*
- "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*
- Depending on the information certain fields are mandatory – *DRIVES Administrator's Manual, p. 37*

### Condition / Evidence

We conducted data analysis to validate the completeness of demographic data collected by the Department to provide permits and licensing to Northern residents.

1. We reviewed the DRIVES **Client data table** and observed the following exceptions:

*Active "Individual" Records Missing Mandatory Information*

| Category | Active | Pending | Total |
|---|---|---|---|
| Date of Birth | 0 | 11 | 11 |
| Gender ID | 0 | 91 | 91 |
| Weight | 170 | 580 | 750 |
| Height | 0 | 579 | 579 |
| Eye Colour | 52 | 573 | 625 |
| Hair Colour | 51 | 574 | 625 |
| Total Unique Records | | | 754 |

*Active "Organization Records" Containing Personal Data*

| Category | Total |
|---|---|
| Date of Birth | 5 |
| Gender ID | 6 |
| Weight | 3 |
| Height | 5 |
| Eye Colour | 4 |
| Hair Colour | 4 |
| Total Unique Records | 7 |

2. According to the DRIVES Administrator Manual, "Government Type ID" is a mandatory field. Out of 9,550 active Organization records in the **Client data table** 1,414 were identified as NULL (no Government Type ID)

3. Within the 366,977 records in the DRIVES **Address data table**, 104,921 records were "Active." Review of the active database highlighted the following concerns:
   - 7 records with a blank address
   - 24 records with a blank postal code

| **Risk/Consequence:** | |
|---|---|
| • DRIVES program may not have up-to-date client information, which may impact eligibility to access services and/or permits.<br>• Demographic data shared across federal/provincial/territorial (FPT) programs may be inaccurate, effecting client's access to services.<br>• Inaccurate data shared across FPT programs may negatively affect the government's reputation. | **Risk Rating:** High<br>**Likelihood:** Almost Certain<br>**Impact:** Moderate<br>**Risk Owner:** Director, Compliance & Licensing<br>Support:<br>• Director, Corporate Services, INF<br>• Manager, Driver & Vehicle Licensing Programs |

**Recommendations:**

1. Send out written instructions to all CSC's and Highway Patrol Staff to ensure the Government Type ID field is marked as N/A in future if not the government ID.

2. Review pending and active files during Supervisor Review at Quality Assurance/Quality Control (QA/QC) process.

3. Create and/or update policies and processes for:
   a. DVLP Policy Manual regarding mandatory characteristic data
   b. Quality Assurance/Quality Control (QA/QC) Process

| **Management Response:** | **Timeline:** |
|---|---|
| 1. Written instructions have been communicated to issuers. Reviewed all Government ID and confirmed all were non-government and amended accordingly. | Complete |
| 2. Pending and active files missing information reviewed and deactivated as required. | Complete |
| 3. Management will create update policies to cover items related to single name entries and to the QA/QC process. | February 29, 2020 |

**CONFIDENTIAL**

August 2, 2017

File: 7820-31-PWS-151-106

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

| | |
|---|---|
| **Management Letter:** | **Technology Service Center, Release and Deployment Management Process** |
| **Review Period:** | **August 1, 2016 to April 30, 2017** |

In August 2016, we started work on your management requested project that was approved by the Audit Committee. The purpose of the project was to provide advice and support to the Technology Service Center's (TSC) development of a release and deployment management (release management) governance framework.

Release management was a process for managing new systems, servers and/or patches (upgrades for software applications and technologies) by scheduling and controlling the movement of releases to the test and live environments. Software patches were necessary to fix or improve existing problems with software that were noticed after the initial release, such as security and specific program functionality. The TSC followed policies and guidelines from the Office of the Chief Information Officer (OCIO) and the ITIL Framework. However, the TSC recognized that they needed to develop in-house direction for their own staff.

In August 2016, we engaged the TSC and advised them to document a Terms of Reference (TOR) that would articulate the purpose and authority of the Change Advisory Board (CAB). The CAB was tasked with oversight of all changes in the

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

GNWT IT production environment under TSC management. We reviewed and provided feedback on the draft TOR and it was finalized and approved by the TSC Director in November 2016 **(Appendix A Refers).** To enhance the TOR, the TSC will be considering adding membership roles and constituting a quorum in their annual review of the TOR.

We conducted a walkthrough with TSC to demonstrate the COBIT 5 Self-Assessment Tool. This tool was an effective and efficient way to conduct self-assessments and determine process capability levels to enhance internal controls. We provided the TSC with access to the tool.

In February 2017, we reviewed and provided feedback on the proposed patch management process flow **(Appendix B Refers)**. We engaged the OCIO to understand the corporate wide governance on patch management and obtained the patch management guidelines and patch management best practice **(Appendix C & D Refers)**.

The TSC has made progress towards building a sound process for release management. The next steps for the TSC would include:

- Documenting and finalizing
    - relevant policies and procedures for each stage of the release management process flow. Guidance to complete this phase may be obtained from the *ITIL Service Transition Processes- Release and Deployment Management.*
    - problem management process flow and related policies and procedures.
- Liaising with the OCIO to ensure that corporate Electronic Information Security Standards were incorporated into policies and procedures.
- Conducting a COBIT 5 self-assessment once all processes and the relevant governance framework had been implemented.

A well planned release management process would enable the TSC to add value to the GNWT by using a consistent approach to delivering change faster, at optimum cost and minimised risk. Although the TSC uses the ITIL framework to deliver service in accordance with minimum standards, the capacity to deliver service needs to be examined in relation to the risk being mitigated for the GNWT. The TSC should formalize and communicate use of the ITIL framework to all stakeholders, to provide a solid foundation to manage people, process and technology.

Once fully implemented, the IAB or an independent contractor could be engaged to provide an independent, objective assessment of the governance framework. Should you require additional information, please feel free to call me at (867) 767-9175, ext. 15215.

Sincerely,

Shahi

T. Bob Shahi<br>
Director, Internal Audit Bureau

c. Mr. Jamie Koe, Comptroller General, FIN
Mr. John Vandenberg, Assistant Deputy Minister, INF
Mr. Dave Heffernan, Chief Information Officer, OCIO
Ms. Laurie Gault, Director, TSC, INF
Mr. Vince McCormick, Director, Corporate Services, INF

APPENDIX A

# **Terms of Reference** for IT Change Advisory Board (CAB) November 8th, 2016

## Background

The IT **Change Advisory Board (CAB)** is an integral part of a defined ITIL change management process designed to balance the need for change with the need to minimize risks. **CAB** is responsible for oversight of all changes in the GNWT IT production environment that are under management of the TSC. These may involve but are not limited to; hardware, software, configuration settings, patches, etc.

## Mandate/Purpose/Objective

The **CAB** supports the IT Change Management Process by recommending approval, or rejecting requested changes and assisting in the assessment and prioritization of changes. This body is generally made up of IT and Business representatives that include: a change manager, user managers and groups, technical experts, possible third parties and customers (if required).

**CAB** offers multiple perspectives necessary to ensure proper decision-making. For example, a decision made solely by IT may fail to recognize the concerns of GNWT business units. The **CAB** is tasked with reviewing and prioritizing requested changes, monitoring the change process and providing managerial feedback.

## Scope

**CAB** is responsible to review and assess any and all business and technical details for all submitted Change Requests (CR). It is the duty of all **CAB** members to ensure they have a clear understanding of the CR and assess risks and cast their vote where required. **CAB** does not provide technical advice to the change team.

## Membership

Chair(s) – TSC Change Manager will chair this board

Members - the **CAB** members will selectively be chosen from IT/IS/IM and business communities to ensure that the requested changes are thoroughly checked and assessed from both a technical and business perspective. **CAB** is not required to meet face-to-face on each requested change, but rather use electronic support and communication tools as a medium. It is however advised that **CAB** meet for reviews of high risk/corporate level changes and a quarterly meeting is scheduled to review history of changes, and discuss any future major changes.

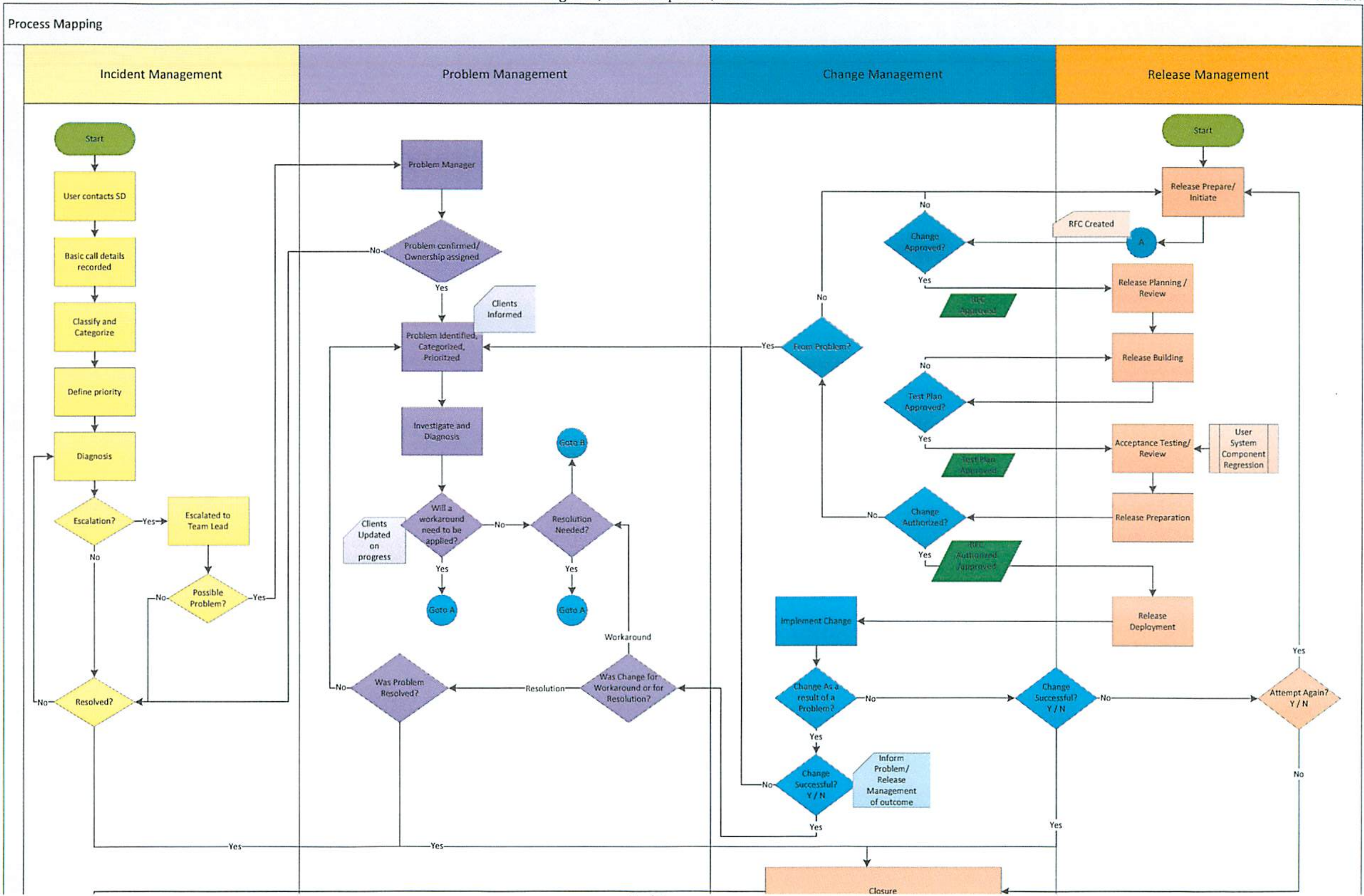
## Authority/Decision making

(**CAB**) offers multiple perspectives necessary to ensure proper decision making is performed. (**CAB**) is tasked with reviewing and prioritizing requested changes, monitoring the change process and providing managerial feedback.

All recommendations regarding proposed changes must be acceptable to voting **CAB** members and consensus is reached or achieved prior to final approval.

2017-PWS-Release & Deployment of Patches
File no: 7820-31-PWS-151-106
August 1, 2016 to April 30, 2017

APPENDIX B



APPENDIX C

## Guideline: GNWT Patch Management

### 1. Introduction

This patch management guideline is intended for all GNWT departments to aid in the scheduling and deployment of operating system security patches. Deploying security patches for known vulnerabilities on a scheduled basis will reduce GNWT's risks and improve program or service stability.

This guideline aligns with the GNWT's Policies and Standards in maintaining appropriate security measures to protect the confidentiality, integrity and availability of our information and assets.

### 2. Purpose

The purpose of this guideline is to document an agreed schedule to update operating system security patches.

### 3. Implementation

Departments should identify an employee to be responsible for scheduling and coordinating patch management tasks with the TSC. This person ideally would be the departments (Information Systems Analyst or Information Systems Manager) as they are likely the central point that would initiate changes like these within your department. If not the person will need to be authorized to schedule patch management activities on your departmental applications with the TSC.

### 4. Patch management recommended process

The approach is provided as a model that a department agrees to a common patching schedule while keeping in mind the resource availability and risk profile of the departmental program or application.

### 5. Prepare a tiered patching server inventory for scheduling

Use the recommended 3 tiers table below for scheduling servers for patching.

| Tier One | Tier Two | Tier Three |
|---|---|---|
| 20(1)(k) [redacted] | [redacted] | [redacted] |
| | | |

### 6. Patch scheduling

Steps for departments implementing a patch management guideline are as follows:

#### a) Preparation

20(1)(k)

- [redacted]

#### b) Patch deployment

- TSC resources apply identified patches to departmental servers based on agreed schedule.

**<u>When a high impacting or critical patch is released by a vendor an emergency</u>**

**patch can be agreed to and deployed that is out of the planned schedule or in a blackout window.**

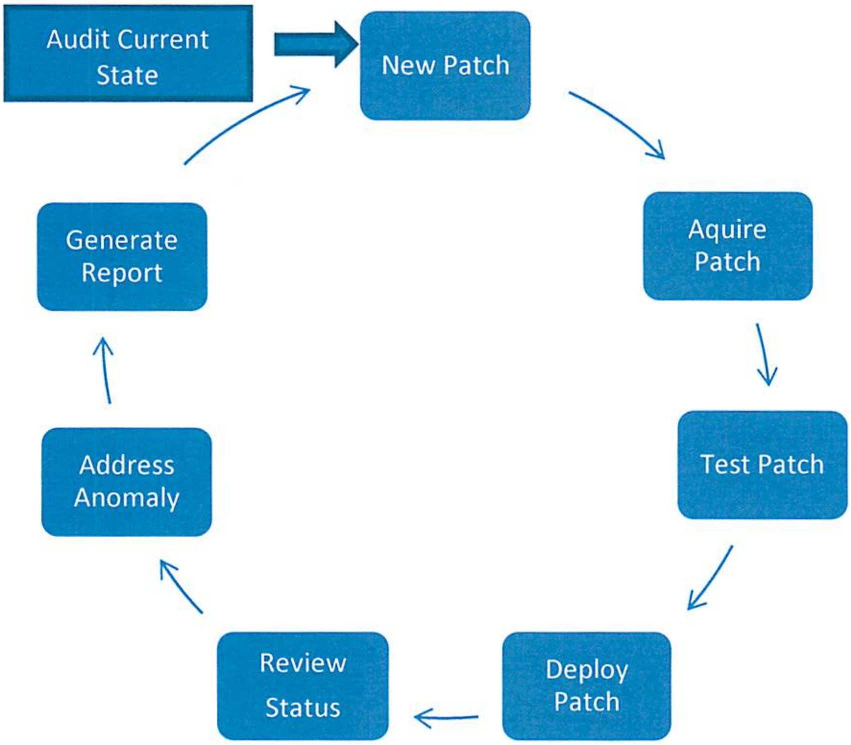
### c) Contingency plan

- If a patch fails to run during implementation, TSC should assess why and resolve, then add the patch to the next patch maintenance schedule.

### d) Reporting

- TSC can provide patching status reports for tracking and reference to the departments, if needed be.

## 7. Suggested best practice flow of patch management



## 8. Role & Responsibility of Patch Management team

| | Responsibility |
|---|---|
| Department | Use the existing TSC departmental inventory for tier schedule. |

| | |
|---|---|
| TSC | Download and deploy identified patches. Verify OS is back online after the patch installation completes. |
| Department | Departmental resources to verify if the patches deployed on their test environment are fit to be deployed to production environment. In case of a problem, the department will notify the TSC to unload the patch and to remove the production server from the patch schedule and assess why the patch is unable to be installed. |
| Department & TSC | Work together to ensure a scheduled patch management program is implemented to address the GNWT's risk and vulnerabilities. |

# A Practical Methodology for Implementing a Patch Management Process

## Executive Summary

Managing the vulnerabilities and security 'holes' in operating systems, applications, databases and other IT assets is fundamental to realizing the opportunities of new technologies and in ensuring that the Government of the Northwest Territories embraces innovative service delivery and new technology safely.

How do we fix a 'hole?' We patch it. Patch management is a method of fixing security vulnerabilities and other system bugs. It involves updating and providing new software to maintain a computer program or its supporting data – usually to either fix or improve it.

### Patching versus Configuration Management

The time between the discovery of an operating system or application vulnerability and the emergence of an exploit is increasingly shorter - sometimes only a matter of hours. This requires systems owners and IT operations professionals to support rapid patch production systems and updating.

However, patching can conflict with configuration management best practices and can cause jeopardize the availability of resources. Patching can break existing systems in the process of installing required security patches and not. Steps involved as follows: identifying, evaluating and applying security patches in a real world environment

Patch management is a subset of the overall configuration management process. This means that there should be in place a strategy for establishing, documenting, maintaining and changing the configuration of all servers and workstations according to their function. Configuration management underlies the management of all other management functions: security, performance, accounting and fault.

A patch management process that includes risk analysis and mitigation strategies, implementation of automated tools, and puts in place a repeatable process to maintain the patch level of all enterprise computing platforms will address all of these guidelines.

A good patch management plan consists of several phases. The plan outlined below consists of seven phases.

### *Phase 1 – Baseline and Harden*

Gather and consolidate inventory data on every server, switch, router, printer, laptop and desktop in the enterprise. Data to be collected should include hostname, location, IP address, operating system and current revision levels of all that needs to be patched.

Each server should also have an indication of it criticality to the enterprise mission. The higher the rating, the more mission critical the system. Factors to consider when determining the mission critical status of a system would include: system role in the enterprise mission, impact on the mission of system down time and time and effort required for disaster recovery. The mission critical status translates into a risk level to the enterprise of the system being unavailable. This risk factor becomes important when making the decision of if, when and how to apply a patch. The servers in an enterprise can be divided into three environments:

§ **Mission critical** – an environment in which even one hour of downtime will have a significant impact on the business service. Examples would be e-commerce sites where downtime can translate into significant lost revenue and consumer confidence.
§ **Business critical** – an environment in which business services require continuous availability, but breaks in service for short periods of time are not catastrophic. Examples would be payroll
processing servers, E-mail servers.
§ **Business operational** – an environment in which breaks in service is not catastrophic. Examples include print servers, file servers, E-mail gateways

**Recommendation**

Many organizations have situations where the responsibility for maintaining the server hardware and operating system falls on one group (TSC) but the maintenance of the applications running on the server are the responsibility of owner department group. In this situation it is vital that proper change management procedures be implemented and adhered to which includes security precautions in place in their environment.

Once the data is gathered it should be documented and distributed to all system owners. Put in place a process to keep the data current.

### *Phase 2 – Develop a Test Environment*

Once the environment is baselined, build a test environment that mirrors the production environment. At a minimum, the test environment should have test servers representing all mission critical applications. Ideally, every type of platform in the enterprise should be represented in the test environment. In many cases, if applications are developed in house there should already be servers that can be used for testing security patches.

It may not be possible to maintain a test environment that mirrors the production environment. In this situation, patches should be deployed to the least critical, easily recoverable servers first. These would be servers without a lot of data or applications that need to be restored. An example would be print servers. These can be rebuilt quickly from registry backups. When installing patches on E-mail servers, update the gateway before the database server.

One cost effective means of establishing a test lab is to use VMware to create a "Lab in a box". While this method won't account for hardware variables in patch testing, it is a good way to test patch compatibility with the OS as well as any applications that are running on production servers. VMware supports Windows as well as Linux operating systems. A replica of the production environment can exist on a single piece of hardware allowing the patch testers to evaluate multiple configurations of operating systems and applications and their interaction with each other before and after patch installation.

### *Phase 3 – Develop Backout / Rollback Plan*

Before any patch is installed, a full backup of all data and server configuration information must be made. Best practices for disaster recovery recommend periodic testing of the restore process to ensure the integrity of the backed up data. Create Emergency Repair disks for all servers after updating. This way, it won't have to be done before the next update. When updating workstations, establish a group of test users who are the first to obtain the new updates. After successful deployment to the test group, expand to the rest of the enterprise. Users should be storing their critical data on network shares and have minimal desktop customization to facilitate rapid restoration from a standard image.

### *Phase 4 – Patch Evaluation and Collection*

Keeping current with hotfixes and updates can be a daunting task. It is important to be able to quickly evaluate which updates are critical, which ones are merely useful and which ones are unnecessary. An automated tool makes this job a little easier by either maintaining a database of monitored systems and their patch status or scanning them on demand. These results are then compared to a database of the ideal configuration and systems needing to be updated are identified. Gartner Group has identified nine functional requirements that should be considered by enterprises that are considering automated solutions for patch management:

1. The solution should be able to create and maintain an inventory of server and desktop systems. It should be able to discover new systems without requiring the distribution of an agent.
2. The automated solution should be able to provide information about installed service packs and patches for the operating system as well as each major installed component.
3. It should be able to evaluate patch prerequisites. This will reduce the labor requirements of patch management.
4. The automated solution should maintain a current, dynamically refreshed inventory of patches and information about them. This will help the enterprise prioritize patch installations based on the criticality from a security perspective.
5. The automated solution should be able to report the patches that are needed by each individual server and workstation.
6. The automated solution should support role-based administration and system grouping. This allows the workload to be distributed among groups of system owners.
7. This may be obvious but automated "patch management tools should provide patch distribution and installation functions, including the ability to automate the installation of patches that require intervention". (Nicolett, p.3)
8. Since Microsoft still dominates the desktop environment, most patch management solutions have greater Microsoft support. That is beginning to

change and as will be described later, some are beginning to add Unix, Linux and even Novell support.

9. There are two types of automated solutions. Agentless architectures rely on scans of target machines to determine their update status. This type is easier to set up and configure but consumes more network bandwidth to push out patches. Agent based systems are more efficient users of network bandwidth and provide more functionality but they are also have higher deployment and maintenance costs. However, effective patch management, especially "with respect to mobile users, is likely to require the functionality of an agent based approach" (Nicolett, p.3). Organizations should leverage as much as possible any established software distribution agents for patch management. This is where all of the preliminary work will pay off. The next three phases can be broken down into 5 steps: receiving information on latest software updates and vulnerabilities; auditing the enterprise for applicable software updates; assessing and authorizing available software updates; deploying authorized software updates within the enterprise in a timely, accurate, and efficient manner; tracking update deployment across the enterprise. (Systems Management Server Version 2.0, Enterprise Software Update management Using Systems Management Server 2.0 Software Update Services Feature Pack, White Paper, p. 5). Tools are available for analyzing the current patched status of systems, downloading available patches from a central database and managing the installation of the patches. Some of these tools are Solaris Patch Manager Tool for SUN Solaris, Ximian Red Carpet Enterprise for Linux, Microsoft Systems Update Services (SUS) and the SUS Feature Pack for Microsoft Systems management Server (SMS) for Windows 2000 and up. These products all maintain a database of systems and installed patches, analyze patch dependencies, deploy approved patches to clients and track patch installation status. Some of them also provide a rollback feature to return to the previous version of the software in case of problems. Microsoft SUS is fairly easy to get up and running in a Windows 2000 environment. The configuration usually consists of two SUS servers. One is used for downloading the patches from the Microsoft web site and deploying them to the test workstations. Once the patch stability is verified, they are copied to the production server and advertised to the clients. Windows 2000 machines with service pack 3 or greater and Automatic Update configured will then download and install the updates according to the settings configured by the administrator. In Active Directory enable domains, the client settings can be deployed through group policy. In non-Active Directory environments, the client settings can be configured through registry changes

deployed via the login script, Windows NT-4 style system policy or SMS if it is available. The limitation of SUS is that it will only distribute patches and updates available from the Windows Update site. These consist of security hotfixes and patches and service packs for the Windows operating system and related components such as Internet Explorer. Enterprises using SMS have the option of employing the SUS Feature Pack for SMS. The SUS Feature pack has a few advantages over straight SUS. It can be used to distribute service packs and updates for Office applications as well as OS updates. It also gives the administrator more control over the distribution schedule as well as tracking the status of the client installations. The SUS Feature Pack uses the HFNETCHK scan agent, developed by Shavlik, to inventory current patch status of client machines. Shavlik sells a GUI version HFNetChk called HFNetChkPro. HFNetChkPro differs from most patch management products in that it doesn't use an agent which makes it easier to install and manage. Like SUS and the SUS Feature pack, HFNetChkPro supports only Windows. PatchLinkUpdate from Patchlink is a cross platform patch management solution. It supports Windows 95 through 2003, Novell NetWare, Unix including Linux, Solaris, AIX andHP-UX. PatchlinkUpdate is an agent based solution and in tests done by eWeek, was the most consistent in deploying patches across the enterprise. Patchlink maintains a database of patches released by OS and application vendors. They conduct additional tests of the patches in their labs before they make the patches available for download. For an additional fee, they will test patches against an image supplied by the customer. For heterogeneous environments, Patchlink Update may be the perfect solution for managing updates. Ximian makes Red Carpet Enterprise which supports only Unix based machines including the Red Hat, Mandrake, SuSE and Debian flavors of Linux as well as Solaris 8 and 9. Red Carpet users subscribe to "channels" to keep track of available updates. This allows users to monitor specific projects or collections of files beyond the standard security updates and bug fixes for essential packages. (Hall Linux Planet Remote workstations are the bane of most administrators. Keeping them current with anti-virus software is enough of a challenge without adding security updates to the mix. Most users are still using slow dial up connections to access the company intranet and they have little tolerance for delays while waiting for software downloads. Some IT organizations spend an inordinate amount of time trying to develop strategies for deploying updates to home based workstations. Other organizations are taking a different approach. They are using products like Citrix Metaframe for their remote users. Citrix is a client server solution where no data is transferred

PUBLIC

between the client and the server. Only keystrokes and video refresh data is sent over the network and all processing occurs on the server side. While this solution doesn't protect the remote clients, it does prevent any potential vulnerabilities present on the client machine from spreading through the network.

***Phase 5 – Configuration management***

After the patch has been tested and is ready to be deployed, the proposed changes to systems and the results of the testing should be documented and approved by system owners. The system owners should be prepared to standby in case disaster recovery steps are required. The helpdesk should be aware of the planned updates, any possible side effects and remediation instructions if users are affected. If automated systems monitoring is active, the appropriate personnel should be notified if any monitored systems will be going offline and triggering alerts. If any adverse events do occur during the deployment, the details of what occurred and on what systems should be documented and incorporated into future testing. And finally, capable personnel should be available to test systems after patch deployment.

***Phase 6 – Patch Rollout***

Once the patch has passed internal testing and configuration management review, it is time to deploy it. If one of the previously described tools is being used to monitor patch status and gather patches from vendors, it can also be used to distribute the patches to clients. Most of the tools have the ability to schedule patch distribution and don't require user intervention so that deployments can be done during off peak hours but even better, no one has to stay late to monitor them. Patching of mission or business critical servers should be done manually during off hours in case disaster recovery plans need to be implemented. If the patch is not an emergency fix, it can be applied during a regularly scheduled maintenance window. Make sure that the maintenance window allows for the recovery process if required. Patching of business operational servers can be accomplished through the use of the same tools as the workstations. Enterprises that don't have access to these tools will have to rely on alternate methods of patch distribution. They can utilize login scripts to deploy patches and free utilities such as HFNETCHK to report on the status. Or they can post the patches to an intranet site and provide users with instructions for installing them.

***Phase 7 – Maintenance Phase – Procedures and Policies.***
Maintaining the enterprise resources at current level is a function of establishing and following documented policies and procedures. Documented can't be emphasized enough because the policies and procedures must be able to survive staff turnover. Below are some guidelines to establishing patch management policies.

1. Designate patch management lead person or team. Ensure that they have support from top management and authority to get the job done.

2. Establish policies for patch updates. Non-critical updates on non-critical systems will be performed on regular scheduled maintenance windows. Emergency updates will be performed as soon as possible after ensuring patch stability. These updates should only be applied if they fix an existing problem that the server is experiencing. Critical updates should be applied during off hours as soon as possible after ensuring patch stability.

3. Establish procedures for checking for the existence of available patches, assessing the applicability of the patches and testing the patches. The more thoroughly the process is documented, the less vulnerable it is to staff turnover and loss of institutional knowledge. Ensure that the testing team contains members who are familiar with every application used in the enterprise.

4. Constantly update the workstation images for new PCs with the latest updates. Make sure that all workstations utilize a standard security configuration and don't prevent authorized access to install updates.

5. Provide regular reports for management. IT personnel can often enjoy more personal freedom if their management knows that they are on top of important issues.

---

**Patch Priority Matrix**

In the table below, specify the names of all the applications used in the company. Under the "Application Criticality" column, specify the application's criticality to the company. In the "High/Moderate/Low Priority Patch" Columns, list the timeframe that patches must be installed in if they fall within each category. Add additional rows if they are required to complete the Priority Patch Matrix below.

| **System/Application** | **Application Criticality** | **High Priority Patch** | **Moderate Priority Patch** | **Low Priority Patch** |
|---|---|---|---|---|
| [Name/Type] | [High/Medium/Low] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] |
| [Name/Type] | [High/Medium/Low] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] | [Immediate/ 1 week/ 2 weeks/ 3 weeks/ 1 month] |

## Policy

1. Vulnerability assessment and system patching will only be performed by designated individuals. These individuals are [name staff members and/or roles].

2. All server, desktop, and laptop systems, including all hardware and software components, must be accurately listed in the IT Department asset inventory to aid in patching efforts.

3. Vulnerability scanning of systems will take place [name frequency/times]. [Company Name] uses the following tools to scan its systems for security vulnerabilities: [list tools used for servers, desktops, and laptops]. [Company Name] systems will be scanned for vulnerabilities with the following frequency:

   - Servers will be scanned [name frequency]
   - Desktops will be scanned [name frequency]
   - Laptops will be scanned [name frequency]

4. The following information sources will be taken as primary authorities on existing and new system vulnerabilities. These sources must be monitored by assigned IT personnel on an ongoing basis.

   - [Name information source]
   - [Name information source]
   - [Name information source]

5. Each vulnerability alert and patch release must be checked against existing [Company Name] systems and services prior to taking any action in order to avoid unnecessary patching. Read all alerts very carefully – not all patches are related to issues or actual system versions present at [Company Name].

6. The decision to apply a patch, and within what timeframe, must be done following the guidelines presented in the Patch Priority Matrix.

7. All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated and the integrity of

the patch verified. All patches must be submitted to an anti-virus scan upon download.

8. New servers and desktops must be fully patched before coming online in order to limit the introduction of risk.

9. New software must be fully patched when installed on GNWT resources to limit the introduction of risk

10. All patches must be tested prior to full implementation since patches may have unforeseen side effects. Describe testing procedure using either a dedicated test network or non-critical machines.

11. A backout plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.

12. Patches will be applied according to the following schedule: Describe patching schedule such that it provides minimal disruption to business activities.

13. Rollout of tested patches will adhere to the following procedure: Describe tiered rollout procedure, including all automated systems used.

14. All configuration and inventory documentation must be immediately updated in order to reflect applied patches. This includes the following documents: List the documents that must be regularly updated to reflect patch installations.

**Enforcement**

Audits will be performed [name frequency] to ensure that patches have been applied as required and are functioning as expected.

**Patch Management Software**
**Automated Patch Management Software for Windows & Mac**

"The use of DC has allowed me to do the job of many employees thus saving us money. I push updates to local and remote employees as well as complete new installs of applications. When there has been vulnerabilities that have surfaced I have been able to quickly deploy the patch across our organization." Patch Management software applications that are popular today, aim at overcoming the vulnerabilities that create security weakness, corrupt critical system data or cause system unavailability. Such software vulnerabilities can otherwise be a nightmare for Network Managers. IT Administrators can't even think of a good solution, without understanding how vulnerable their systems are. This makes them to constantly look out for a solution that scans for network vulnerabilities, identifies missing security patches and hotfixes, applies them immediately and mitigates risk; and not just a patch deployment software.

Desktop Central's agent-based solution handles every aspect of Windows, Mac and Third Party Application patch management like System discovery, identifying the required Windows Microsoft updates, Mac Updates and Third Party Applications detail, deploying relevant patches, hotfixes, security updates, and patch reports to make network administrators job simple. Network Managers can opt for this completely automated patch management software solution and don't have to worry about patching Windows systems ever. Desktop Central's Patch Management solution works for both Windows Active Directory and Workgroup based networks. Also, you can manage both Microsoft and ***Non-Microsoft Patches*** using a single Patch Management application.

Refer to Securing Windows Desktops to see the ways to enhance desktop security using Desktop Central.

Features

- Uses a hosted Patch Database at Manage Engine site to assess the vulnerability status of the network
- Completely automated Patch Management Solution for both physical and virtual assets.
- Solution from detecting the missing patches/hotfix to deploying the patches
- Patch based deployment - Deploy a patch to all the systems applicable
- System based patch deployment - Deploy all the missing patches and hotfixes for a system
- Provision to test and approve patches prior to bulk deployment
- Automatic handling of patch interdependencies and patch sequencing
- Reports on System vulnerabilities, Patches, OS, etc.
- Provides an update of the patch deployment status.
- Supports both Microsoft and Non-Microsoft Patches.

- Supports Anti-Virus Definition Updates for Microsoft Forefront Client Security Software.

### Automatic System Discovery

The Desktop Central solution performs automatic discovery of Windows systems using Active Directory. Administrators can choose the systems that have to be managed using Desktop Central. The Desktop Central agent that is installed in the managed systems performs the actions initiated from Desktop Central Server. This agent is responsible for vulnerability assessment scan and patch deployment.

### Online Vulnerability Database

The Online vulnerability Database is a portal in the ManageEngine site, which hosts the latest vulnerability database that has been published after a thorough analysis. This contains the list of all Microsoft Windows updates that are available. This database is exposed for download by the Desktop Central Server situated in the customer site, and provides information required for patch scanning and installation.

The Desktop Central Server located at the enterprise (customer site) scans the systems in the enterprise network, checks for missing and available Windows patches against the comprehensive vulnerability database, downloads and deploys missing Microsoft patches and service packs, generates reports to effectively manage the patch management process of the enterprise.

### Vulnerability Assessment Scan

Dekstop Central scans all the systems for missing Windows patches in operating systems and applications and the level of vulnerability is reported. These missing Windows patches are identified from the local vulnerability database, which is periodically synchronized with the external online vulnerability database maintained by ManageEngine.

### Approval of Patches

Most often the patches have to be deployed in a test environment to ensure that they are error-free and stable, before they are rolled out to the entire network. Also, in cases where you have a team of system administrators, you can ensure that the patches tested by one team can directly be approved for deployment. This saves a lot of time, which can be utilized for other critical tasks.

### Patch Deployment

Dekstop Central takes care of deploying the patches based on missing Microsoft patches or system vulnerability. Once deployed, the agent applies the relevant Windows patches in the system and security updates and updates the status in Desktop Central. The installation process can be scheduled from patch settings option.

### Patch Reports

Patch reports gives details about system vulnerability level, missing Windows patches, applicable Windows patches, task status, etc. All these reports are available as pdf or in printer friendly versions.

### Severity Based Patch Management

Desktop Central facilitates administrators to create and configure severity levels for the missing patches. This helps them to deploy patches based on severity. So they need not evaluate system health and vulnerability status based on a common list of missing patches. This helps them to be more accurate and specific to identify the significant patches which are missing and rate it based on severity of the missing patch. This not only tailors their day to day patch management activity but also enhances the patch management process to be more accurate and reliable.

### Automated Patch Management Solution

Using Desktop Central's Automated Patch Deployment feature, you can automate your patch-management process. This feature enables you to deploy patches that are missing in the computers in your network automatically. You can automate the following tasks using the Automated Patch Deployment feature:

- Scanningcomputers periodically to identify missing patches
- Identifying missing patches and downloading them from the vendors' Web sites
- Downloading patches that you require and creating tasks related to patch deployment
- Downloading patches that you require automatically and installing them on to specific computers

All the levels of patch-deployment automation mentioned above can be specified fora specific set of client systems. You can choose to have different levels of automation for different sets of client systems. The process of deploying patches automatically depends on the level of automation you choose.

Microsoft Forefront Client Security Definition Updates

Anti-Virus definition updates is quite crucial for enterprises that run Microsoft Forefront Client Security software to protect their networks from the attack of trojans and viruses. With malicious code on the increasing side, Network Administrators need to keep an eye on these frequent definition updates to avoid any possible mishaps. However, you can simplify the process using Desktop Central's Patch Management options. Using Automated Patch Deployment you can schedule the frequency to scan the systems for virus definition updates and specify the action to be performed on successful completion of the scanning.

## Six steps for security patch management best practices

**Step 1:** Develop an up-to-date inventory of all production systems, including OS types (and versions), IP addresses, physical location, custodian and function. Commercial tools ranging from general network scanners to automated discovery products can expedite the process (see Resources, below). You should also inventory your network periodically.

**Step 2:** Devise a plan for standardizing production systems to the same version of OS and application software. The smaller the number of versions you have running, the easier your job will be later.

**Step 3:** Make a list of all the security controls you have in place--routers, firewalls, IDSes, AV, etc.--as well as their configurations. Don't forget to include system hardening or nonstandard configurations in your list of controls. This list will help you decide how to respond to a vulnerability alert (if at all). For example, let's say you learn that OpenSSH has a vulnerability that may allow a buffer-overflow attack, but from your list of controls you know you don't allow the SecSH protocol through your firewall. If nothing else, that knowledge gives you more time to react.

**Step 4:** Compare reported vulnerabilities against your inventory/control list. There are two key components to this. First, you need a reliable system for collecting vulnerability alerts. And second, you need to separate the vulnerabilities that affect your systems from those that don't. Some companies have staff dedicated to managing this process; others use vulnerability reporting services.

**Step 5:** Classify the risk. Assess the vulnerability and likelihood of an attack in your environment. Perhaps some of your servers are vulnerable, but none of them is mission-critical. Perhaps your firewall already blocks the service exploited by the vulnerability. In general, to classify and prioritize the risk, consider three factors: the severity of the threat (the likelihood of it impacting your environment, given its global distribution and your inventory/control list); the level of vulnerability (e.g., is the affected system inside or outside perimeter firewalls?); and the cost of mitigation and/or recovery.

**Step 6:** Apply the patch! OK, so now you have an updated inventory of systems, a list of controls, a system for collecting and analyzing vulnerability alerts and a risk classification system. You've determined which patches you need to install. Now comes the hard part: deploying them without disrupting uptime or production. Fear not, there are several tools that can help you with the actual patch process (see Resources, below). Evaluate these tools in terms of how well they fit your environment and budget. In some cases, manual patch maintenance may be more cost-effective. But in most cases--particularly for multiple servers or server farms distributed across multiple locations--some type of automated patch system will more than pay for itself.

Vulnerability and patch management isn't easy. In fact, in today's computing environment, it's a never-ending cycle. But by following these general steps, you'll be way ahead of the curve when the next worm comes knocking at your network door.

===□□□**Patch Management**

- Maintain security, at least, by implementing a patch management process (automated or manual)
- Monitor security intelligence resources to become aware of vulnerabilities and exposures.
- Classify the patches according their severity.
- Test the patches on a production similar environment and document the findings; implementation.

https://www.sans.org/reading-room/whitepapers/sysadmin/proposal-managing-system-security-patches-enterprise-network-311

Government of Northwest Territories Gouvernement des Territoires du Nord-Ouest

**CONFIDENTIAL**

June 28, 2019

File: 7820-20-GNWT-151-135

MR. PAUL GUY
DEPUTY MINISTER
INFRASTRUCTURE

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

## A. SCOPE AND OBJECTIVES

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

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

## B. BACKGROUND

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

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

- Regulatory Revenues such as Airport landing fees, Inspection Services – Boiler
- Program Revenue such as Canadian Air Transport Security Authorization Agreement
- Revolving Funds Net Revenue such as Marine Transportation Services Revolving Fund
- Service and Miscellaneous such as Airport concession, Sale of surplus assets.

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

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

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

## C. SUMMARY OF KEY FINDINGS AND RECOMMENDATIONS

The audit report, *"Department of Infrastructure, Revenue Process Audit Report,"* made several observations and recommendations specific to Infrastructure (**Schedule I refers**).

In assessing Infrastructure's revenue processes, the contractor determined that there was:

- Compliance with FAM 605 (recording revenue)
- Compliance with IB 620.01 (collection of accounts receivable)
- Non-compliance with IB 610.01 (rationale for the fee charged).

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

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

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

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

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

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

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

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

## D. ACKNOWLEDGEMENT

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

T. Bob Shahi
Director, Internal Audit Bureau
Finance

# SCHEDULE I

## DEPARTMENT OF INFRASTRUCTURE

## REVENU AUDIT PROCESS AUDIT REPORT

# 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.<br>Regulated rates are reviewed every five year as per FMB direction.<br>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. |
| **IB610.01 Rationale for Fees Charged**<br>GNWT Departments and Public Agencies are to ensure that fees are collected, safeguarded, and accounted for.<br>A rationale for each fee charged must be kept available for audit purposes.<br>The rationale in support of each fee charged must include:<br>- pricing details;<br>- the price/rate basis, including direct, indirect, and accounting and system costs; and,<br>- the time period for cyclical fee reviews.<br>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. | **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.<br>*See Observation 9 below.* |
| **IB 620.01 Collection of Accounts Receivable**<br>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.<br>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.<br>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.<br>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:<br>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. | **Compliant** | Revenues on account are invoiced and the debtor is provided 30 days from the date of invoice to make payment.<br>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.<br>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. |

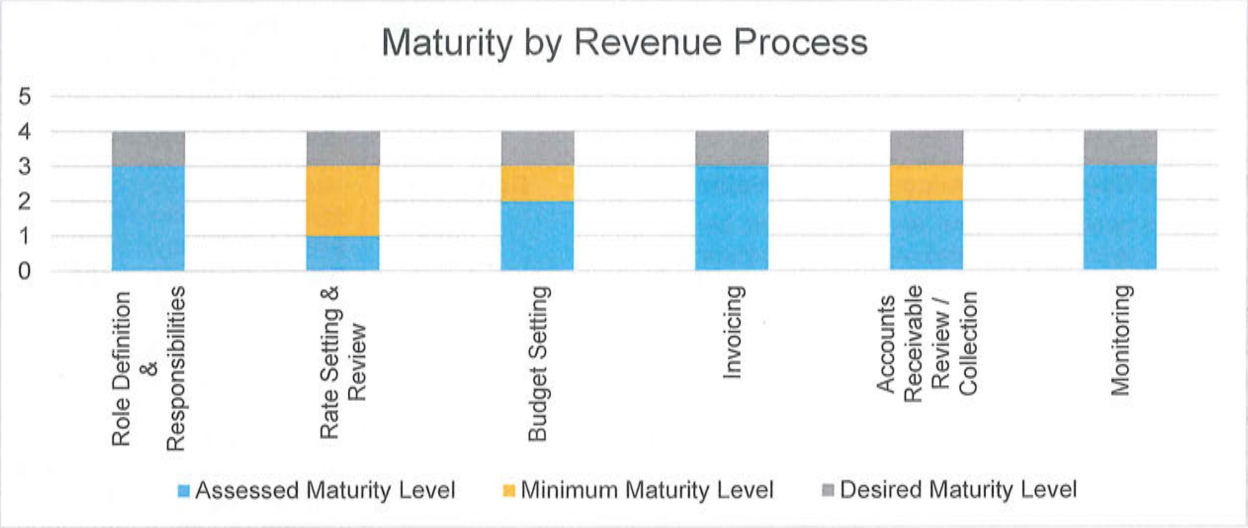
### Maturity Rating Considering GNWT Internal Control Capacity Model

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**<br>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 | • Job descriptions exist for the positions outlined above under departmental background as responsible for the department's general revenue functions.<br>• Job descriptions include responsibilities related to specific general revenue cycle components.<br>• Job descriptions reviewed by Crowe have all been updated within the last two years. |
| **Rate Setting & Review**<br>The department reviews rates on a set periodic basis to ensure rates are current and new revenue sources have been considered. | Ad Hoc | • Majority of rates and fees are regulated and are charged in accordance with regulations.<br>• Regulated rates and fees are reviewed every five years per FMB direction. Rationale for fees is not documented.<br>• Non-regulated rates and fees are not reviewed on a set periodic basis and policies and processes are not documented.<br>• 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 |
|---|---|---|
| | | *See Observation 1, 2 and 3.* |
| **Budget Setting**<br>The department clearly defines and documents the revenues expected for each year with explanations for any material changes from prior years. | Repeatable | • Clarity on roles and responsibilities exists for INF Financial Planning.<br>• INF Financial Planning prepares the operating budget with revenue estimates from Corporate Services.<br>• Budget of revenues is based on prior year estimates and actuals with input from program managers not on statistical information.<br>• Assumptions and rationale for estimates are not documented.<br>*See Observation 4.* |
| **Invoicing**<br>The department ensures that invoices are prepared in a timely manner, and are accurate and complete. | Defined | • Invoices are not issued for the majority of the department's revenue streams because payment is received at the time of service.<br>• Processes are in place to record revenues received in cash or by online payment at the time the service is provided.<br>• Processes are in place to ensure all revenues earned are recorded as revenues for revenues received by cheque or direct payment.<br>• Processes are fully documented for each significant revenue stream and are reviewed annually and updated where necessary. |
| **Accounts Receivable Review / Collection**<br>The department monitors receivables on a set periodic basis and ensures that follow-up takes place if revenues are not received as expected. | Repeatable | • The department has a "Finance General" email established for emails from FESS and a department representative has been assigned.<br>• The department has a process for addressing emails received from FESS regarding unallocated receipts by cheque.<br>• 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.<br>• The policy the department has for addressing emails received from FESS regarding unallocated receipts |

| Revenue Process Area | Assessed Maturity Level | Findings and Comments |
|---|---|---|
| | | by cheque does not include specific procedures to be taken by department staff.<br>• The department has verbally communicated the procedure for sending all direct payment notifications to Department of Finance - Financial Reporting.<br>• The department reviews and responds to unclaimed deposit emails from Department of Finance - Financial Reporting.<br>• The procedures to be taken when an unclaimed deposits email is received from Department of Finance - Financial Reporting have not been established and documented.<br>• 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.<br>• "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.<br>• The department understands the role and responsibility of the Collections unit.<br>• Policies mentioned above are reviewed annually and updated where necessary.<br>*See Observations 5, 6 and 7.* |
| **Monitoring**<br>The department reviews variances between budget and actual revenues received on a set periodic basis. Follow up takes place if revenues are | Defined | • 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 |
|---|---|---|
| not being received as expected. | | • Explanations for variances are documented.<br>• Variance reports are reviewed and provided to Management Board Secretariat.<br>• 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:

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) 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) 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. |

| | |
|---|---|
| satisfy this recommendation. | Implement for next business planning cycle (2021-22). |

## 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:

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) 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<br>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.<br>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<br>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.<br>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<br>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 | Est. September 30, 2019. |

| | |
|---|---|
| include the Department of Finance. | |
| 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) 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 A

# Financial Administration Manual

| | Department | Financial Reporting / Collections | MBS / FMB | Comptroller General |
|---|---|---|---|---|
| **Establishment of Fees** | • Deputy Head responsible to set fees and charge for licenses, permits and services rendered to the public<br>• Minister responsible to advise the FMB of the introduction, change or removal of a fee within 60 days | - | MBS may issue directives respecting financial management or administration of a Public Agency | • May approve Interpretation Bulletins associated with this policy<br>• Establish and maintain systems and procedures to ensure the integrity of GNWT financial records and accounting systems<br>• Establish/ maintain systems and procedures to ensure public money is collected and accounted for, internal controls are in place |
| **Rationale for Fees Charged** | • Ensure fees are collected, safeguarded, and accounted for<br>• Rationale for each fee must be kept for audit purposes | - | - | |
| **Recording Revenue** | • Deputy Head of dept. responsible to ensure revenues accurately recorded in a timely manner in accordance with GAAP | - | - | |
| **Receipt of money** | • Responsible for collection and management of all A/R | Engage courts or outside collection agency | - | |

# GNWT Revenue Process Audit
# Roles & Responsibilities

## Appendix B

## Shared Services Agreement

| | Department | FESS | Financial Reporting / Collections | MBS / FMB | SAM Team | Comptroller General |
|---|---|---|---|---|---|---|
| **Estimates (Budgets)** | • Prepare | - | - | • MBS review/ FMB approval | • Support | • Appointed by Minister of Finance<br>• Maintain systems and procedures with respect to the integrity of government financial records and accounting systems<br>• Ensure compliance by GNWT departments, Public Agencies and other reporting bodies with accounting policies and practices<br>• Manage Consolidated Revenue Fund and Public Accounts. |
| **Variance reports** | • Prepare | - | - | • MBS review/ quarterly to FMB | • Support | |
| **Invoices** | • Request/ set up | • Acct. approval | - | - | • Maint. | |
| **Cash Payment** | • Process in-dept. receipts | • Process all other receipts | - | - | • System support | |
| **Cheque Payment** | • Provide coding | • Process/ post | - | - | • System support | |
| **EFT Payment** | • Provide invoice/ coding | • Post | • Process | - | • System support | |
| **A/R Mgmt** | • Follow-up <90 days; monitoring ongoing | • Stmt. sent to customer | • Follow-up >90 days; external collections; court | - | • System support | |
| **Training** | • Dept. training | • FESS training | • FR/ collection training | • MBS training | • SAM-based training | |

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

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

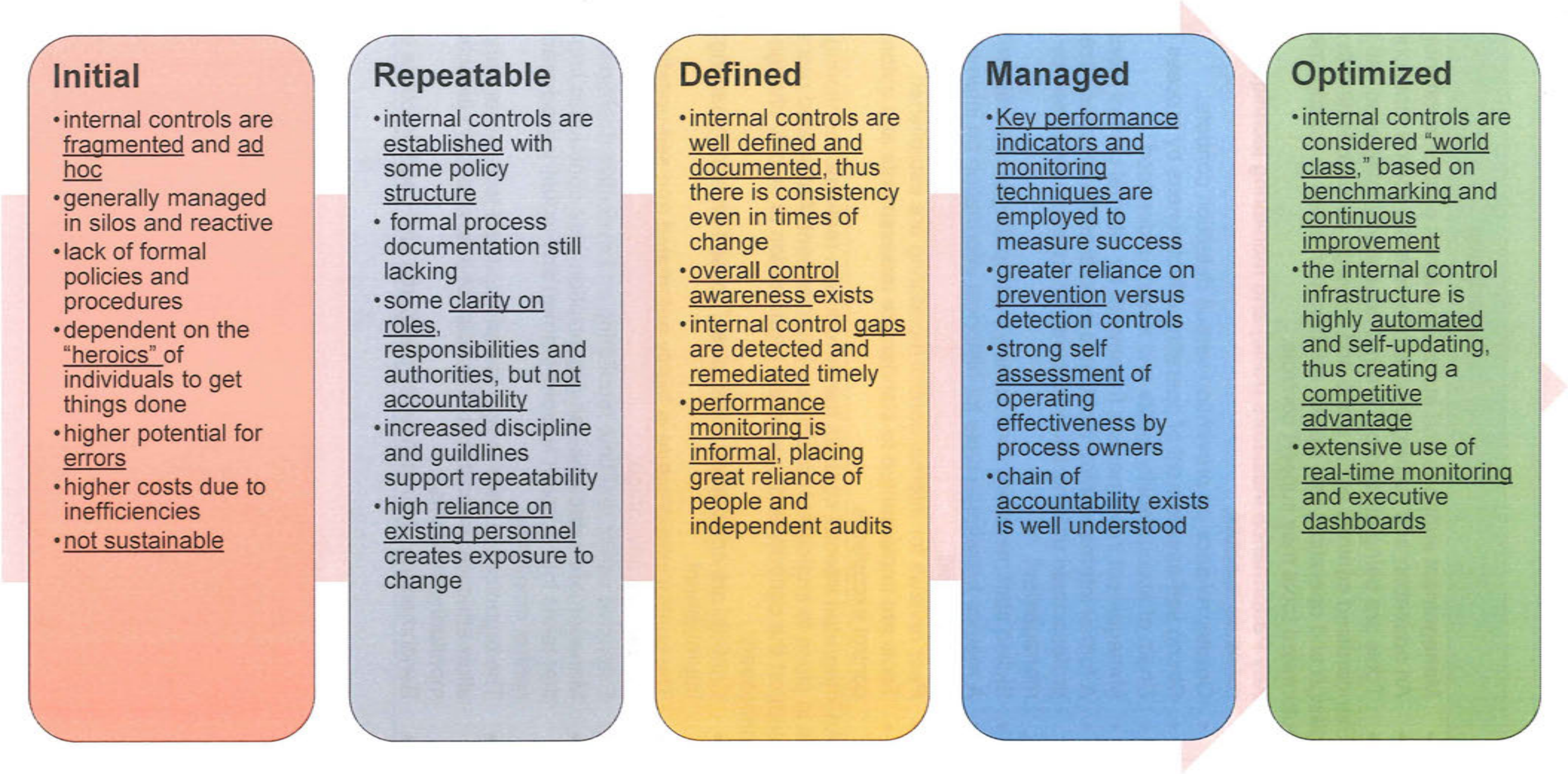
# APPENDIX C

## INTERNAL CONTROL CAPACITY MODEL

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

| Deliverable | Description |
|---|---|
| 0 - Non-existent | • The organization lacks procedures to monitor the effectiveness of internal controls.<br>• Management internal control reporting methods are absent.<br>• There is a general unawareness of internal control assurance.<br>• Management and employees have an overall lack of awareness of internal controls. |
| 1 - Initial/Ad Hoc - Unreliable | Unpredictable environment for which controls have not been designed or implemented.<br>• Controls are fragmented and ad hoc.<br>• Controls are generally managed in silos and reactive.<br>• Lack of formal policies and procedures.<br>• Dependent on the "heroics" of individuals to get things done.<br>• Higher potential for errors and higher costs due to inefficiencies.<br>• Controls are not sustainable.<br>• Individual expertise in assessing internal control adequacy is applied on an ad hoc basis.<br>• Management has not formally assigned responsibility for monitoring the effectiveness of internal controls. |
| 2 - Repeatable - Informal | Controls are present but inadequately documented and largely dependent on manual intervention. There are no formal communications or training programs related to the controls.<br>• Controls are established with some policy structure.<br>• Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan.<br>• Formal process documentation is still lacking.<br>• Some clarity on roles and responsibilities, but not on accountability.<br>• Increased discipline and guidelines support repeatability.<br>• High reliance on existing personnel creates exposure to change.<br>• Internal control assessment is dependent on the skill sets of key individuals. |
| 3 - Defined - Standardized | Controls are in place and documented, and employees have received formal communications about them. Undetected deviations from controls may occur.<br>• Controls are well-defined and documented, thus there is consistency even in times of change.<br>• Overall control awareness exists.<br>• Policies and procedures are developed for assessing and reporting on internal control monitoring activities.<br>• A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT managers.<br>• Control gaps are detected and remediated timely.<br>• Performance monitoring is informal, placing great reliance on the diligence of people and independent audits |

| Deliverable | Description |
|---|---|
| | • Management supports and institutes internal control monitoring.<br>• An education and training program for internal control monitoring is defined.<br>• Tools are being utilized but are not necessarily integrated into all processes. |
| 4 - Managed - Monitored | 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.<br>• Key Performance Indicators (KPIs) and monitoring techniques are employed to measure success.<br>• Greater reliance on prevention versus detection controls.<br>• Strong self-assessment of operating effectiveness by process owners.<br>• Chain of accountability exists and is well-understood.<br>• Management implements a framework for internal control monitoring.<br>• A formal internal control function is established, with specialized and certified professionals utilizing a formal control framework endorsed by senior management.<br>• Skilled staff members are routinely participating in internal control assessments.<br>• A metrics knowledge base for historical information on internal control monitoring is established.<br>• Peer reviews for internal control monitoring are established.<br>• Tools are implemented to standardize assessments and automatically detect control exceptions. |
| 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.<br>• Controls are considered “word class”, based on benchmarking and continuous improvement.<br>• The control infrastructure is highly automated and self-updating, thus creating a competitive advantage.<br>• Extensive use of real-time monitoring and executive dashboards.<br>• Management establishes an organization wide continuous improvement program that takes into account lessons learned and industry good practices for internal control monitoring.<br>• The organization uses integrated and updated tools, where appropriate, that allow effective assessment of critical controls and rapid detection of control monitoring incidents.<br>• Benchmarking against industry standards and good practices is formalized. |



### Initial

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

### Repeatable

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

### Defined

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

### Managed

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

### Optimized

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