Privacy Management Policy – Compliance Audit

Final Report

Fiscal Year (2016 – 2017)

June 2, 2017

Yukon
Executive Council Office
Government Internal Audit Services

GAM 2.27 – Privacy Audit

Table of Contents

List of Acronyms

ATIPP – Access to Information and Protection of Privacy

CIM – Corporate Information Management

ERM – Enterprise Risk Management

GAM – General Administration Manual

GIAS – Government Internal Audit Services

HPW – Department of Highways and Public Works

HSS – Health and Social Services

ICT – Information and Communications Technology

IIA – The Institute of Internal Auditors

IPC – Information and Privacy Commissioner

IRMC – Information Resources Management Committee

IT – Information Technology

OIPC – Office of the Information and Privacy Commissioner

PI – Personal Information

PIA – Privacy Impact Assessment

PO – Privacy Officer

PSC – Public Service Commission

RFP – Request for Proposals

YG – Yukon Government

1.0 Executive Summary

1.1 Introduction

Governments occupy a privileged position in the community, because they have significant legislative powers to require citizens to hand over personal information. In order to receive services, individuals have no choice but to share their information. Yukon Government therefore needs to meet a higher standard of privacy practice to maintain the trust of its citizenry.

The sensitivity of personal information and its growing impact on privacy is important to recognize. Developments in mobile technology and social networking have turned personal information into a tradeable commodity. Data points that are individually innocuous can be enormously powerful and revealing when aggregated, which is the essence of Big Data. Both the public and private sectors are using Big Data for purposes beyond the initial reason for collecting the information. So long as private data has a value there will be a market for those acquiring it and a market for those protecting it.

1.2 Why we completed this audit

The *Access to Information and Protection of Privacy Act* (ATIPP) was passed in 1995, proclaimed in July 1996, and revised status of Yukon in 2002. The access to information portion (Part 2) was implemented immediately following, including the appointment of departmental ATIPP Coordinators; however, the privacy piece (Part 3) was not really addressed until October, 2015, when the Privacy Management Policy (GAM 2.27) was approved.

The *ATIPP Act* defines personal information and specifies how it is to be collected, used, retained, and disclosed. Unfortunately there could be unnecessary collection and/or retention of personal information within YG, resulting in a certain level of risk. While the Information and Privacy Commissioner (IPC) is there to monitor and to address any complaints, a privacy breach could have a significant impact on the government's reputation, carry potential liability, and be costly to remedy.

1.3 Objectives

The objective of this audit was to assess the compliance of the Yukon Government, all government departments, with the Privacy Management Policy (GAM 2.27) by:

- Assessing each department against the requirements included in the policy;
- Establishing a comprehensive understanding of the current implementation status within the government;
- Identifying gaps in privacy management that need to be addressed; and
- Identifying lessons learned/best practices that could be used by departments (see Appendix B).

1.4 Conclusion

GIAS recognizes that Yukon Government is at an early stage of the implementation of the policy, and that progress is being made. However, the success of GAM 2.27 depends on the support provided by the departments and the capacity of resources within the Corporate Information Management (CIM) office. Thus far, the leadership role played by HPW (CIM) is showing positive results. Momentum needs to be maintained in order to fill out the gaps that have been identified (see 1.5 below).

1.5 Summary of main findings

Highways and Public Works corporate leadership:

- Created the Privacy Impact Assessment (PIA) tools and the Privacy Breach Reporting Form being used by the departments, and which are now mandatory for all YG employees.
- On-line Privacy training is being developed and will be mandatory for all YG employees in 2017.
- In general, CIM is in compliance with GAM 2.27.

Strength of Health & Social Services:

- HSS is the only department with a clear set of policies and procedures relating to the purpose and authority for collection, use, and disclosure of personal information; also, requirements for notification and consent.
- HSS is also the only department to outline exactly how members of the public may access and/or request a correction of their personal information, and make a complaint.
- 90% of employees have completed the mandatory *HIPMA* training and signed a Pledge of Confidentiality afterwards.

Engagement by the departments:

- The majority are lacking a comprehensive set of policies and procedures relating to sections 29 to 36 of the *ATIPP Act*, and none of the 12 departments across YG has successfully completed an inventory of personal information/PI Map.
- 5 out of 12 departments report not using any standard privacy clause as part of contracts with third party service providers.
- 58% of Privacy Officers' (PO) primary jobs are not linked to information management; the PO responsibilities were spelled out in the HPW Deputy Minister's memo, May 2016.

Communication is lacking:

- The role of the departmental Privacy Officer has not been adequately communicated within YG.
- 10 out of 12 (83%) of departments do not readily provide information to members of the public about their rights regarding privacy of personal information and how they may file a complaint. The Privacy Advisory Committee is working on a webpage that will provide all of the names and contact numbers for the departmental Privacy Officers.

1.6 Action taken

HPW has created policies on collection, use and disclosure of private information as well as a complaints policy for all departments and made them available at end of March 2017. A mandatory training course has been launched in March 2017; attendance is tracked and a certificate is issued after successful completion of the course.

HPW prepared the standardized and guidance contractor template which has not yet been approved.

1.7 Recommendations, Management Response and Action Plan

Recommendation	Management Response /Action	Target Date	Position(s) Responsible
1. Deputy Ministers must ensure that their Privacy Officer has the right skills and knowledge to fill out the roles and responsibilities; participate fully in the Privacy Advisory Committee, and ensure GAM 2.27 is operationalized.	Agree. 1) HPW will define the requisite skills and knowledge to fulfill the role and responsibilities of departmental Privacy Officer for Deputy Ministers. 2) Deputy Ministers will ensure their departmental staff work with their Privacy Officers to fulfill their obligations under GAM 2.27 Departmental Privacy Officers will report to their Deputy Minister on progress in fulfilling obligations under GAM 2.27 3) HPW, through the Privacy Advisory Committee, will produce a report for the Deputy Ministers on the status of privacy management activities within each department.	July 2017 May 2017 September 2017	HPW, ICT – Privacy Office Deputy Ministers and Privacy Officers HPW, ICT – Privacy Officer
2. The public has user-friendly access to their rights and how they can enforce them.	Agree. 1) The ATIPP Office has created a "Privacy Complaints" page on the ATIPP website. 2) The ATIPP Office has created a "Privacy Complaint Policy". 3) The ATIPP Office will create a "Privacy Management" page on the ATIPP website for government. This page will make privacy policies and documents available for the public.	May 2017 May 2017 July 2017	HPW, ICT – Privacy Office HPW, ICT – Privacy Office HPW, ICT – Privacy Office

3. Target dates are being fixed to complete the PI Map, to ensure that any privacy information is in compliance with Sections 29 to 36 of the *ATIPP Act*.	Agree. Departments' Privacy Officers complete PI Maps for new programs or activities, as per the PI Map policy as and when a new program or activity commences. 1) Departments will begin to identify programs that hold "confidential" information; "protected" information; and "internal" information, as per "Personal Information Classification Guidance". 2) Departments will begin inventorying their information assets for programs which were identified to have "**confidential**" personal information. Completed PI Maps will be submitted to the ATIPP Office. 3) Departments will begin inventorying their information assets for programs which were identified to have "**protected**" personal information. Completed PI Maps will be submitted to the ATIPP Office. 4) Departments will begin inventorying their information assets for programs which were identified to have "**internal**" personal information. Completed PI Maps will be submitted to the ATIPP Office.	May 2018 May 2019 May 2019 May 2020	Program Manager & Department's Privacy Officer Program Manager & Department's Privacy Officer Program Manager & Department's Privacy Officer Program Manager & Department's Privacy Officer

I approve the above Management Response and Action Plan

Signed by the A/Deputy Minister,

Deputy Minister

A/DM HPW

I recommend this Management Response and Action Plan for approval by the Audit Committee

Signed by the Director and Chief Audit Executive, GIAS

Approved by Audit Committee on **June 16, 2017**

2.0 Scope and methodology

The Audit Committee approved in April 2016 a horizontal compliance audit of privacy. The period covered by the audit is November 2015 (the month following approval of GAM 2.27 on October 27, 2015) to November 2016. GIAS has examined the work done by departments during this time.

The audit examined compliance with the Privacy Management Policy (GAM 2.27) by all departments and centred on the most actively engaged departments in the handling of personal information. Together, Education, HSS, Justice (Correctional Services), PSC, and Highways & Public Works account for the majority of YG's registered personal information holdings. These departments are responsible for activities which collect, use and disclose the most voluminous and sensitive sets of personal data.

This audit was conducted following the IIA Standards for the Professional Practice of Internal Auditing. The audit criteria (see Appendix A) were developed as per GAM 2.27, and the Guidance for Public Bodies on Accountable Privacy Management (published January, 2015, by the Office of Yukon's Information and Privacy Commissioner). These criteria were agreed upon with the authority responsible to assist departments (HPW) and the authority responsible for health information (HSS). As the *ATIPP Act* is scheduled to be reviewed in 2017, the timing was appropriate to assess the implementation of GAM 2.27 and identify any gaps that need to be addressed.

A documentation review of the implementation processes and information available for each department was included in the audit. In addition, a brief phone survey was conducted over the course of two days to test a random sampling of employees government-wide. As GIAS wanted to have a level of 80% assurance (with a 6% margin of error), it was estimated that a total of 111 employees would need to be contacted. After downloading all employees from the YG staff directory, the phone numbers were sorted by department. A random number generator was then used to choose which numbers to call within each department (for confidentiality purposes, names were not recorded).

3.0 Background

The purpose of the *ATIPP Act* is to make public bodies more accountable to citizens and to protect personal privacy. Part 3 of the *Act* outlines purposes for which personal information may be collected, how it is to be collected, accuracy, a citizen's right to request a correction, and protection, retention, use, and disclosure.

In October 2015, the Yukon Government approved the Privacy Management Policy (GAM 2.27). This policy outlines the implementation process for Part 3 (as above) and makes privacy protection a priority for the government. The purpose of the policy is "to apply authorities and responsibilities to YG departments in the management and protection of personal information, referred to as Privacy Management (PM). Privacy management is essential for protecting Yukoners' personal information, including personal health information, as required under the *ATIPP Act* and *Health Information Privacy and Management Act (HIPMA)*."

The *HIPMA* was passed in December 2013 and came into force when the regulations were completed, August 31, 2016. Health & Social Services is responsible for developing regulations and standards for personal health information under *HIPMA*. All custodian departments must follow the standards required by *HIPMA.*

The Information and Privacy Commissioner (IPC) is responsible for monitoring how the *ATIPP Act* is administered, to ensure that its purposes are achieved. Highways and Public Works (HPW) provides corporate guidance and leadership on the Act, issues guidance documents, standards, and training materials to assist departments in delivering and adhering to corporate information privacy policies.

Limitations:

GIAS did not conduct any testing regarding the collection, use and disclosure of personal information because no mapping has been done by any of the departments. GIAS did not feel it was its role to look at files and tell departments what they should be collecting, or how to protect the information, as there could be duplication with IPC roles and responsibilities.

The Department of Finance reported that it has no resources to put towards implementing GAM 2.27 at this time.

4.0 Observations and findings

4.1 Documentation

GIAS generally noticed that documentation is not at the level expected.

4.1.1 – Personal Information Mapping (Criteria #1)

None of the 12 departments across YG has successfully completed an inventory of personal information/ PI Map.

None of the 12 departments across YG has completed a PI Map, with the exception of those introducing a new program using the Privacy Impact Assessment (PIA) tool, which requires a mapping exercise (please refer to Criteria#4, p10). The map is meant to support sections 29 to 36 of the *ATIPP Act*.

Consequently, the Department of Highways and Public Works is unable to identify, government-wide, a) the personal information in the custody or control of YG program areas, b) the purpose for the collection, use and disclosure of this information, and c) the sensitivity of this information.

Without the mapping, there is no standard to apply by which departments can know what information they are actually collecting, using, storing, and distributing about the citizens of Yukon. It is quite possible that the government is collecting information that it should not be collecting, which decreases efficiency without benefits to anyone on either side.

4.1.2 – Privacy Policies and Procedures (Criteria #2)

The majority of departments are lacking a comprehensive set of policies and procedures relating to the purpose and authority for collection, use, and disclosure of personal information.

The majority of departments are lacking a comprehensive set of policies and procedures relating to the purpose and authority for collection, use, and disclosure of personal information. Only Health & Social Services (HSS) is very clear on this point, having developed its own corporate policy manual.

On requirements for notification and consent, HSS was able to provide a clear policy. HSS is also the only department to outline exactly how members of the public may access and/or request a correction of their personal information. This information is available on the website, including a form to fill out for request to access.

No department submitted a document explaining how the accuracy of personal information is to be guaranteed, as required by the *Act*. Regarding retention, destruction, or disposal of personal information, the Department of Education has a policy specific to the disposal of student school work. No other department provided any relevant policy.

HPW and ECO have policies in the area of how personal information will be secured, including administrative, physical and technological controls. The Maintenance Enforcement Program at Justice recently prepared (2016) a policy to ensure the security of personal information in response to an IPC investigation. Others (Environment, Education) have documents which describe how to manage paper and/or records – but not personal information.

All departments are using the Breach Protocol and the Reporting Form developed by HPW to demonstrate how a privacy breach will be managed. Corporate Information Management (CIM) reports that they have not been notified of any privacy breach. No incident reports have been submitted as of November 30, 2016.

The Department of Education has distributed an IPC pamphlet with information about making a complaint. When asked for documentation, none of the other departments provided anything with regards to how privacy complaints will be managed. EMR specifically mentioned the OIPC website, but does not provide a link from its own YG webpage.

There is a risk of inconsistency, within the departments and government-wide, on how personal information is managed. As citizens become better informed about their rights, the number of complaints may increase.

4.1.3 – Contractor (Service Provider) Management (Criteria #3)

5 out of 12 departments report not using any standard privacy clause as part of contracts with third party service providers. Over half of all departments (7/12) specifically report using either the standard Front End contract template or the HPW template.

The Procurement Support Centre supplied a copy of Term #3 in the RFP template (out of 32 General Terms & Conditions) which deals with confidentiality of data and information gained while performing the contract work; it does not specify *personal* information, however. The word 'Confidential' may include but is broader than just Privacy.

The Department of Finance submitted the 10 standard Terms & Conditions which does not contain any clause regarding privacy of information. This is applied to sole-source contracts (contracts created directly from Front End), which means that only RFPs will have the Confidentiality clause.

The Department of Tourism & Culture submitted an Agreement on Commissioned Photography & Video which states that, "Personal Information is collected for the purpose of administering the Department of Tourism & Culture Photography Policy and protecting the rights of government, employees, contractors, and photograph subjects as per the *Copyright Act* and other legislation. For inquiries about this collection of personal information contact […] the Records Officer."

There is a risk that contract service providers are not instructed how to address personal information, which may impact on Yukoners' trust in their government.

4.1.4 – Risk Management Tools (Criteria #4)

Starting on November 4, 2016, privacy breach reporting and the completion of Privacy Impact Assessments (PIAs) are now mandatory for all YG employees.

A Global Note was sent on behalf of HPW on November 4, 2016, stating that privacy breach reporting and the completion of Privacy Impact Assessments (PIAs) are now mandatory for all YG employees.

All departments reported using the corporate PIA tools, which are for new programming only – or significant changes to an existing program. A total of 20 PIAs have been submitted for review from a variety of departments since March 2015 (some of these are only partially completed and currently being worked on). The e-Health projects from HSS made use of an outside consultant who was approved to work with his own template.

HPW encourages the practice to require the Office of the Information and Privacy Commissioner (OIPC) to provide comments on each PIA. This translates into a back-and-forth review process between the OIPC and CIM before approval signatures are provided by the Deputy Minister, or a designate.

As new programs now require a PIA to be completed, and the OIPC is part of the process, and CIM will be auditing privacy management plans, this means the risk for management tools should be mitigated for any new programs.

4.1.5 – Training (Criteria #5, 6)

There is no formal training provided specific to privacy, except in the case of Health & Social Services, and no attendance is being recorded/ tracked.

There is no formal training provided specific to privacy, except in the case of Health & Social Services, and no attendance is being recorded/ tracked. HSS provides its own mandatory comprehensive Privacy and Confidentiality training based on *HIPMA*; other departments touch on *ATIPP* during their orientation sessions for new employees and at other informal gatherings – however, the emphasis is on access to information and not privacy. Some optional Breach training sessions (12 in total) were provided in 2016 by HPW, but no attendance records were kept by either CIM or by the departments.

At HSS, 90% of employees have completed the mandatory *HIPMA* training and signed a Pledge of Confidentiality afterwards. However, until the mandatory on-line Privacy training is completed by all YG staff (projected for 2017), GIAS cannot say with certainty that employees understand their responsibilities for handling personal information within their public service role. At this time, the majority of YG employees are not aware of GAM 2.27 (refer to survey results below).

Up to now, there is a risk that employees who required training did not get it. If people are lacking the knowledge needed to do their jobs, then personal information could be inadequately handled.

Phone Survey Testing

Over the course of two days a brief phone survey of a random sampling of employees was conducted to test privacy awareness government-wide. This survey supports the results for Criteria #14, roles and responsibilities of YG employees. One hundred and eleven (111) calls at a confidence level of 80% were made in total, and the questions were as follows:

1) Are you aware of GAM 2.27, the Privacy Management Policy?
2) Do you know who the Privacy Officer is for your department? (If so, what is the person's name?)

Limitations: 2 people declined to answer the questions, whereas some who said 'Yes' to being familiar with GAM 2.27 may possibly have been thinking of the *ATIPP Act* instead. Some employees replied 'Yes' to the question of knowing their Privacy Officer but then gave the wrong name (23%).

GAM 2.27 and the names of the Privacy Officers have not been adequately communicated within YG.

The overall result for YG as a whole was that 47% of those asked are indeed aware of GAM 2.27, whereas 53% are not. There is a large discrepancy in awareness by department, with the lowest figure being 25% and the highest figure being 80%. Therefore, the Privacy Management Policy could be better communicated to the departments.

Regarding the second question, the department with the best score was where 50% of respondents were able to answer 'Yes' and then accurately name the Privacy Officer. In three (3) separate departments, 100% of employees asked answered 'No', they are not able to identify their Privacy Officer. Five departments landed between 80 and 95% of employees surveyed unable to identify the person in this role.

Overall, 8 out of 12 departments scored a rate of 20% or less respondents able to answer 'Yes' to the question, demonstrating that the role of the departmental Privacy Officer has not been adequately communicated within YG. There is a risk that government-wide, employees will not handle personal information appropriately as they are not familiar with GAM 2.27 and/or do not know who to ask for help. If citizens' personal information is mismanaged, it could impact negatively on the government's reputation.

4.1.6 – Roles and Responsibilities

The implementation of GAM 2.27 by all the parties involved is advancing. The risk of breach incidents could be mitigated with HPW/CIM engagement. However, if departments are not careful regarding the management of personal information, there could be a negative impact on the government's reputation.

The Deputy Minister (Criteria #11)

Deputy Ministers have appointed Privacy Officers who have information management knowledge regarding privacy requirements in 58% of the cases. Most of the DM responsibilities are still a work in progress.

As government-wide privacy management policies and practices are not yet complete within YG, this area remains a work in progress. Deputy Ministers are responsible for ensuring that any and all contractors delivering a service or program for their department comply with the department's privacy management plan. As this plan is not finalized, it would appear that contractors have not been made aware of it.

Deputy Ministers must ensure that employees are trained in privacy management and protection principles. However, consistent training practices on the topic of Privacy have not been implemented across YG (please refer to Criteria#5 & 6).

All Deputy Ministers appointed a Privacy Officer. However, 42% of these are people whose regular positions are not directly related to information management and do not have the knowledge to answer questions or provide advice regarding privacy requirements as per the *ATIPP Act*. Given that the job of Privacy Officer has been added to the role of each employee's regular position, what is the real expectation from each department regarding priority of privacy work? In some cases, the Privacy Officer position was given to the person fulfilling the ATIPP Coordinator role.

Deputy Ministers are responsible for appointing the Privacy Officers. There were no job descriptions made available to them, prior to the Privacy Management Policy (GAM 2.27) and the Memorandum from the DM of HPW dated May 11, 2016 which lists the various responsibilities of the Privacy Officer.

Deputy Ministers have the option to delegate the approval of PIAs and privacy management plans to a designate. In at least one department, it is the ADM signing off on the final version.

Department of Highways and Public Works (Criteria #12)

In general, CIM as part of HPW is in compliance with GAM 2.27

HPW hosts the Corporate Information Management (CIM) office, which ensures there is corporate guidance on the *ATIPP Act*. CIM recruited an Access & Privacy Analyst in October 2014. Starting in 2015, this Analyst began to coordinate work on Part 3 of the *Act*, which had not been addressed by the departments.

In general, HPW (corporate) is in compliance with GAM 2.27. There are only two areas where improvements are needed:

- CIM is in the process of developing and delivering the privacy management program across YG, Criteria#12(a). As the program is still under development, CIM cannot ensure that departments comply. Consequently, there is also no auditing of privacy management plans or reporting on progress and it is too early for GIAS to assess this Criteria (#12, h).
- CIM has not had occasion to review departments' incident management processes and ensure implementation as no breaches have been reported to date; therefore, GIAS cannot assess Criteria#12(f). Incident reporting is now a mandatory requirement as per the corporate Privacy Breach Reporting Policy, and CIM is organized in order to respond.

Based on risk assessment, CIM decided to first address training on Privacy Impact Assessments (PIAs) for new programs, as well as the Breach protocol. The Personal Information Mapping is part of the PIA process (but will only be done for new programs). On-line Privacy training for those who collect, create or access personal information is being developed and will be mandatory. This training should be completed in 2017 and attendance will be tracked.

Action Taken

HPW has created policies on collection, use and disclosure of private information as well as a complaints policy for all departments and made them available at end of March 2017.

HPW prepared the standardized and guidance contractor template which has not been approved yet.

The Privacy Officer (Criteria #13)

Privacy Officers are involved in the PIA process and are participating in the Privacy Advisory Committee. The PO job has been added to the role of each employee's regular position and they need to rely on the GAM 2.27 which lists their responsibilities. The name and role of the PO are not being adequately communicated to all employees within the department.

The PIA process is mandatory as of November 2016, which means that Privacy Officers (PO) should be engaged in risk assessment for all new programs. The degree of involvement of the Privacy Officer varies from department to department; however, they are consistently involved in the process. As per CIM, some PIAs were started before GAM 2.27 came into effect.

The Privacy Officer is responsible for submitting draft and completed PIAs to CIM, although in practice it could be someone else – often the program manager. As there is no dedicated role within departments for the PIA function, the contact person varies based on who is actually writing the assessment. Privacy Officers are generally consulted on the review, after the initial stages. The Privacy Officer is required to oversee the collection of information for the PI map; however, this work has not yet begun across YG, with the exception of mapping included in any PIAs which were submitted to CIM.

Following the breach reporting protocol, Privacy Officers must ensure that any information incidents that have a likelihood of significant harm are disclosed to HPW – however, there have been no information incidents reported as of November 30, 2016. No reporting and audit requirements were fulfilled (refer to Criteria#12(h)).

All Privacy Officers are participating in the work of the Privacy Advisory Committee. The Committee's mandate, as it relates to GAM 2.27, is "to review and comment on proposed tools, guidance, standards and policies." [Committee Terms of Reference] It would appear, however, that the Privacy Officers are not adequately communicating this work to the other employees in their departments. According to the results of our phone survey, most YG employees are not aware of GAM 2.27, nor are they informed about the name of their departmental Privacy Officer.

Departments were not able to provide a job description specific to the Privacy Officer in 100% of the cases. 42% (5/12) submitted a main job description belonging to the person assigned the PO role, which mentions general responsibility for compliance with *ATIPP* legislation. In only 2 cases were there any further details regarding Privacy. The other 58% (7/12) did not send any job description whatsoever – although Department of Justice reproduced the responsibilities as outlined by the DM of HPW in his

May 2016 memorandum. This Deputy Minister's memo was also requesting that departments submit the name of their appointed PO; therefore GIAS assumes that there were no Privacy Officers prior to this date.

Employees (Criteria #14)

Tools are being put in place to support employees regarding their role in protecting privacy.

Employees cannot comply with their department's privacy management program and/or plan as there is no clear program or plan in place across YG, with the exception of HSS. Neither can they commit to increasing their awareness of privacy requirements and best practices, as there has been no formal Privacy training provided. Until the mandatory on-line training is complete (in 2017), there will be no government-wide engagement on GAM 2.27 (please refer to the Phone Survey, p11-12).

4.2 Communication/Reporting

10 out of 12 (83%) of departments do not readily provide information to members of the public about their rights regarding privacy of personal information. As the public becomes more cognizant of these rights, there is the possibility that individual complaints could increase and negatively impact levels of trust, along with the government's reputation.

4.2.1 – The Privacy Management Program (Criteria #7)

The privacy management program is not complete across YG and there is no information available to members of the public, with the exception of info about *HIPMA* shared by HSS through the local papers and the distribution of pamphlets.

4.2.2 – Rights under the ATIPP Act (Criteria #8)

Only HSS and HPW clearly inform members of the public about their rights under the *ATIPP Act*. There is a link on the first page of the departmental website at HPW leading users directly to the relevant information. HSS has produced a comprehensive pamphlet about citizens' rights under *HIPMA*, as well as large ads in at least two local newspapers.

10 out of 12 (83%) of departments do not readily provide information to members of the public about their rights. The Department of Economic Development has an informative brochure for businesses, but not for members of the public; Education includes a clause at the bottom of school Field Trip consent forms regarding *ATIPP* and the collection of personal information, but nothing on their website. Some departments list *ATIPP* under the Acts & Legislation section of their government website, but it is not always easy to access/find.

4.2.3 – Privacy related complaints (Criteria #9)

HSS gives a phone number on the departmental website to call for complaints. The HPW website does not provide any detail other than the number for the ATIPP office within the department. ECO reported that this information is available on the IPC website, while all other (9) departments failed to provide any documentation showing the way in which members of the public are informed about how privacy related complaints will be handled.

The Privacy Advisory Committee is working on a webpage to appear on the main YG site which outlines when and how members of the public may file a complaint, along with all the names and contact information for the departmental Privacy Officers.

4.2.4 – Information and Privacy Commissioner (Criteria #10)

No department, other than HSS, is informing members of the public that they can make a complaint to the Information and Privacy Commissioner.

5.0 Conclusion

Overall the audit found that, subsequent to the approval of GAM 2.27, progress has been made with the support of the Corporate Information Management office (CIM). However, as the *Act* stands since 2002, it is clear that Privacy has not been given the same priority as Access to Information, and there are areas which could be improved throughout. Deputy Ministers, or their delegate(s), will need to be more cognizant of how individual information is handled within their departments. Judicious use of this information, and a demonstrable respect for privacy, is fundamental to ensuring transparency and preserving the trust of the citizens of Yukon.

Appendix A: Table of audit criteria, sources and methodology used.

Criteria	Methodology
1. Personal Information Map (Inventory). Department of Highways & Public Works is able to identify: 1.a) the personal information in YG program areas' custody or control (amount, categories, number of individuals whose personal information it holds, and location) 1.b) the purpose for the collection, use and disclosure of the personal information 1.c) the sensitivity of the personal information	Document review
2. Privacy Policies and Procedures include: 2.a) the purpose and authority for collection, use and disclosure of personal information 2.b) requirements for notification and consent 2.c) how to ensure accuracy of personal information 2.d) how to facilitate individual access to and correction of personal information 2.e) retention and destruction or disposal of personal information 2.f) how personal information will be secured, including administrative, physical and technological controls 2.g) how a privacy breach will be managed 2.h) how privacy related complaints will be managed	Document review
3. Contractor (service provider) Management Procedures and controls are in place to ensure contractor/service providers comply with the privacy management control program	Document review
4. Risk Management Tools Risk assessment tools and mitigation processes are used, such as privacy	Document review

Criteria	Methodology
impact assessments (PIAs) and security threat risk assessments (STRAs)	
5. Training Employees participate in mandatory privacy awareness training **6. Training** Employees understand their responsibilities for handling personal information within their public service role	Document review Survey
7. Communication/Reporting Information about the privacy management program is available to the public **8. Communication/Reporting** Individuals are informed about their rights under the ATIPP Act **9. Communication/Reporting** Individuals are informed about how their privacy related complaints will be handled **10. Communication/Reporting** Individuals are informed they can make a complaint to the Information and Privacy Commissioner	Document review
11. Roles and Responsibilities **The Deputy Minister:** 11.a) Ensures the department has adopted privacy management practices and implemented government-wide policies 11.b) Ensures employees are trained in privacy management and protection principles 11.c) Ensures contractors delivering a service or program for the department comply with the privacy management plan 11.d) Appoints a Privacy Officer	Document review

Criteria	Methodology
11.e) Establishes responsibilities for privacy within the department 11.f) Approves PIAs and privacy management plans prepared within the department **12. Roles and Responsibilities** **Department Highways & Public Works**: 12.a) Develops and delivers the privacy management program across YG, through the Corporate Information Management office (CIM) 12.b) Provides direction to departments and advisory services on requirements under the ATIPP Act 12.c) Supports the development and resourcing of staff training to encourage a privacy-aware corporate culture 12.d) Develops and distributes privacy management policy guidance, templates and standards to departmental Privacy Officers to ensure a consistent approach 12.e) Collaborates with department staff to develop PIAs and privacy management plans, reviewing final versions and providing written recommendations (if required) to the Deputy Minister prior to approval 12.f) Reviews departments' incident management processes and ensures they are implemented 12.g) Acts as the corporate point of contact and on-going liaison with the Information and Privacy Commissioner (IPC) 12.h) Ensures departments comply with the privacy management program, auditing privacy management plans and reporting on progress 12.i) Makes information about the privacy management program available to the public 12.j) Acts as Chair of the Privacy Advisory Committee **13. Roles and Responsibilities**	

Criteria	Methodology
The Privacy Officer: 13.a) Works with program areas to develop and implement privacy management plans that include risk assessments, as per the PIA operational policy 13.b) Provides draft and complete PIAs to the Corporate Information Management office (CIM) 13.c) Oversees submitting information for the personal information map to Highways and Public Works for approval 13.d) Ensures that information incidents are reported to HPW 13.e) Ensures reporting and audit requirements set by HPW are met 13.f) Participates in the Privacy Advisory Committee **14. Roles and Responsibilities** **Employees:** 14.a) Comply with the privacy management program and the privacy management plan in place within their department 14.b) Commit to increasing awareness of privacy requirements and best practices, and training on privacy protection (as required)	Survey

The Auditee reviewed and accepted the suitability of the criteria used in the audit.

Appendix B: Lessons Learned from Health Canada and Correctional Service Canada

From Health Canada – Audit of Privacy Practices (December 2012)

The audit focused on privacy practices at Health Canada and compliance with the framework set out in the federal *Privacy Act*. The following lessons learned have been written to be suitable for Yukon Government.

Core components of a privacy management framework:

- Organizational commitment (buy-in from the top)
- Clearly defined roles and responsibilities for privacy compliance
- Training and education requirements
- Breach and incident management response protocols
- Reference to privacy policy and risk assessment tools
- Mechanisms for oversight and review

Governance

The development and implementation of a privacy management framework is necessary to guide and enforce good practices department-wide. This will preserve a department's reputation in the eyes of Yukoners as a trusted custodian for sensitive information.

Employees need to know what is expected of them with regards to the handling and protection of personal information. A show of commitment from the top ensures clear expectations around privacy from senior management. One coherent framework for use across all branches is beneficial.

Overlapping/shared responsibilities amongst several points of contact for privacy may lead to misunderstandings and weak accountabilities.

Clear roles and responsibilities for the management of personal information are required in order to enforce accountability and clarify decision-making authorities.

Risk Management

An effective privacy impact assessment (PIA) process identifies and mitigates privacy risks. PIAs are essential to strategic decision-making and risk management.

PIAs are a core component of the privacy management framework. This comprehensive model can successfully evaluate the effects of a particular program on an individual's privacy. A mandatory screening process to identify new programs or projects involving personal information will ensure that assessments get done.

Formal privacy training is essential to ensure a culture of privacy awareness and protection.

Responsibility for making employees aware of policies, procedures and legal obligations lies at the top management level (Deputy Ministers/Heads or their delegates). Training should include privacy breach protocols, and should be continuous and available year-round. Dedicating resources to specific training requirements for program areas most actively involved in the handling of personal information is beneficial.

Internal Control

Collection of personal information should be limited to only what is demonstrably necessary.

Documented administrative controls provide employees at all levels with the appropriate knowledge. A review of standard forms and procedures (regarding the collection, use, disclosure and retention of personal information) should be done where significant changes to programs have been made.

Adequate resources must be allotted for the provision of privacy advice and support within Yukon Government.

It is important to have the right level of resources for providing privacy advice and support. It is also necessary to have the position across departments and the Yukon Government consistently staffed and properly provisioned.

From Correctional Service Canada (October 2006)

If a privacy management framework is fragmented, it will lead to gaps and, in some cases, unclear direction.

Sharing of data, results and analyses regarding privacy breaches or lessons learned with the staff should reduce the occurrence of similar breaches within the organization.