Office of the Information and Privacy Commissioner for Nova Scotia

Privacy Management Program
Gap Analysis - Getting Started
For Smaller Public Bodies & Municipalities

Introduction:

This document was developed by the Information and Privacy Commissioner for Nova Scotia[1] and is intended to assist smaller public bodies and municipalities with beginning to develop and implement a robust privacy management program. An overview of the elements of a robust privacy management program is contained in *Privacy Management Program At-a-Glance* on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: https://oipc.novascotia.ca. This gap analysis document provides detailed information about some of the elements of a privacy management program. The goal of this gap analysis is to identify shortcomings in the program with a view to creating a foundation for a robust privacy management program. The gap analysis results should then be used to develop a privacy oversight and review plan that addresses each of the identified gaps.

Once you have completed this gap analysis and implemented all of the required changes you should review the full Privacy Management Program Gap Analysis for public bodies, also available on our website at: https://oipc.novascotia.ca.

Contact Us:

If you have questions or comments with respect to this document please contact us at:

Office of the Information and Privacy Commissioner for Nova Scotia
PO Box 181
5670 Spring Garden Road, Suite 509
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*.

Instructions: This gap analysis tool begins with a Gap Analysis Summary document (page 3). When complete this will serve as a one page summary of the results of your review. Your goal is to develop a visual gap analysis by assigning red, yellow or green to the outcome of your assessment for each of the elements of your privacy management program.

Step 1: Begin by assessing the two categories of building blocks: organizational commitment and program controls. For each category we have provided a list of essential elements. Record your evaluation of each element by describing the current state of affairs in your municipality. Be as honest and critical as you can. The goal here is to accurately state your municipality's current status.

Step 2: For each requirement score your municipality's compliance on a scale of 1 to 3. Feel free to give partial points. Ratings are explained on page 3.

Step 3: Record the overall score then assign a colour to it and record the colour on the summary sheet at page 3. Colour ratings are explained on page 3.

Step 4: Once you have completed all of your ratings, review the summary sheet at page 3 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

Sample - Gap Analysis Summary	
PMP Requirement	**Overall Gap Analysis Rating**
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	2.2
b. Privacy Officer	2.6
c. Privacy Office	1.3
d. Reporting	2.5
Building Blocks – Program Controls	
a. Personal Information Inventory	2.8
b. Policies	2.0
c. Risk Assessment Tools	2.0
d. Training and Education Requirements	1.6
e. Breach and Incident Management Protocols	2.4
f. Service Provider Management	2.4
g. External Communication	1.5
Oversight and Review Plan	
a. Develop Oversight and Review Plan	2.0

Gap Analysis Summary	
PMP Requirement	**Overall Gap Analysis Rating**
Building Blocks – Organizational Commitment	
a. Buy-in from the Top	
b. Privacy Officer	
c. Privacy Office	
d. Reporting	
Building Blocks – Program Controls	
a. Personal Information Inventory	
b. Policies	
c. Risk Assessment Tools	
d. Training and Education Requirements	
e. Breach and Incident Management Protocols	
f. Service Provider Management	
g. External Communication	
Oversight and Review Plan	
a. Develop Oversight and Review Plan	

Gap Analysis Ratings & Colour Ratings for Summary Chart

Rating	Colour code	Rating Description
1.0 – 1.9	Red	Little to no evidence of compliance – documented or in practice
2.0 – 2.5	Yellow	No documented evidence of compliance but some evidence of effective practice in compliance or documented practice requirement with only limited evidence of implementation.
2.6 – 3.0	Green	Documented and substantial practical compliance.

Building Blocks – Organizational Commitment		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
a. Buy-in from the Top	**Overall Rating**	
• Senior management endorses the program controls (policies, risk assessments, training) and provides necessary resources.		
b. Privacy Officer	**Overall Rating**	
• A senior manager is assigned responsibility for overseeing the municipality's compliance.		
c. Privacy Office	**Overall Rating**	
• Role of the privacy office is defined and staff foster culture of privacy within the organization.		
• Staff work to ensure that privacy protection is built into every major function involving the use of personal information.		
d. Reporting	**Overall Rating**	
• There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured and whether it is functioning as expected.		
• The reporting program has documented reporting structures.		
Building Blocks – Program Controls		
a. Personal Information Inventory	**Overall Rating**	
• The organization has completed a personal information inventory or equivalent.		
b. Policies	**Overall Rating**	
• Four key policies are in place: (i) how to access and correct personal information. (ii) retention and disposal of personal information. (iii) responsible use of information and information technology. (iv) privacy breach management policy.		

Building Blocks – Program Controls continued		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
c. Risk Assessment Tools	**Overall Rating**	
• Privacy risk assessments are required for all new projects involving personal information and on any new collection, use or disclosure of personal information.		
d. Training and Education Requirements	**Overall Rating**	
• All employees receive general privacy protection training.		
• Privacy training is mandatory for all new employees.		
• Individuals who handle personal information directly receive additional training specifically tailored to their roles.		
• Training and education are recurrent and the content of the program is periodically revisited and updated to reflect changes.		
e. Breach and Incident Management Response Protocols	**Overall Rating**	
• There is a procedure for the management of personal information breaches.		
• There is a person responsible for managing a breach.		
f. Service Provider Management	**Overall Rating**	
• Contractual or other means are in place to protect personal information.		
• Transborder data flows and requirements of the foreign regime are addressed in service provider arrangements.		
g. External Communication	**Overall Rating**	
• Individuals are aware of how to access and correct their personal information.		
• Individuals are aware of how to complain including the right to submit a complaint to the Information and Privacy Commissioner.		

Oversight and Review Plan		
List of Expectations	**Evidence of Compliance**	**Gap Rating**
a. Develop Oversight and Review Plan	**Overall Rating**	
• The Privacy Officer develops an oversight and review plan on an annual basis that sets out how the privacy management program's effectiveness will be monitored and assessed.		
• The plan establishes performance measures.		
• The plan includes a schedule of when all policies and other program controls will be reviewed.		