Privacy

ABOUT PRIVACY

AKNOWLEDGEMENT: AUMA acknowledges the work undertaken by the Risk Management and Governance Board Directors Advisory Group, Canadian Institute of Chartered Accountants, (now known as the Chartered Professional Accounts of Canada) on which this paper is based.)

One of the risks a municipality needs to manage is "privacy risk". Municipalities are familiar with the Freedom of Information and Protection of Privacy Act and, as "local Professional bodies" under the Act, have designated FOIP Contacts. Other organizations, such as AUMA, are covered by the Personal Information Protection Act. Personal information privacy risk management involves assessing how your municipality and any related organizations are complying with those Acts.

CICA has suggested that, in addition to personal information privacy, a reasonable expectation of privacy in Canada might also include:

- Personal privacy (for example, physical and psychological privacy)
- Privacy of space (for example, freedom from surveillance)
- Privacy of communication (for example, freedom from monitoring and interception).

A municipality's privacy risk involves personal information stored in hard copy and electronically. Security of a web site also needs to be considered.

UNDERSTANDING PRIVACY RISK

1. What personal information about residents, electors, taxpayers and employees does your municipality collect?
2. What personal information is used in carrying out your municipality's activities?
3. What personal information is obtained from, or disclosed to, third parties? (For example, if any of your municipality's activities are outsourced)
4. What is the impact of the Freedom of Information and Protection of Privacy Act on how your municipality carries out its activities? of the Personal Information Protection Act on how any related organizations carry out their activities
5. How do your strategic and business plans address the privacy of personal information?

IMPLEMENTING A PRIVACY COMPLIANCE REGIME

6. To what degree is your CAO actively involved in the development, implementation and/or promotion of privacy measures in your municipality?
7. Who is your FOIP Contact?
8. Does your FOIP contact have clear authority to oversee your municipality's information handling practices?
9. Are adequate resources available for developing, implementing and maintaining a privacy compliance system?
10. What privacy policies has your municipality established related to the collection, use, disclosure and retention of personal information?
11. How are the policies and procedures for managing personal information communicated to the employees? To members of Council?
12. How are employees with access to personal information trained in privacy protection?
13. Are the appropriate documentation and manuals required by the system fully developed?

MANAGING PRIVACY RISK

14. What specific objectives have been established regarding compliance with your municipality's privacy policies and the relevant legislation?
15. What are the consequences of not meeting these objectives?
16. To what extent have appropriate control measures been identified and implemented?
17. How is the effectiveness of the privacy control measures monitored and reported?
18. What mechanisms are in place to deal effectively with failures to apply your municipality's privacy policies and procedures?

OBTAINING PRIVACY ASSURANCE

19. Would your municipality benefit from a comprehensive assessment (audit) of the risks, controls and business disclosures associated with personal privacy information?
20. Has your municipality considered obtaining independent advice with respect to both online and offline privacy?