Office of the Auditor General / Bureau du vérificateur général

FOLLOW-UP TO THE 2010 AUDIT OF INTERNET AND EMAIL USAGE POLICIES AND PROCEDURES

2012

SUIVI DE LA VÉRIFICATION DES POLITIQUES ET PROCÉDURES CONCERNANT L'UTILISATION DES SERVICES D'INTERNET ET DU COURRIEL DE 2010

Table of Contents

EXECUTIVE SUMMARY i
RÉSUMÉ iii
1 INTRODUCTION 1
2 FINDINGS OF THE ORIGINAL 2010 AUDIT 1
3 STATUS OF IMPLEMENTATION OF 2010 AUDIT RECOMMENDATIONS 6
4 SUMMARY OF THE LEVEL OF COMPLETION 9
5 CONCLUSION 9
6 ACKNOWLEDGEMENT 9

EXECUTIVE SUMMARY

Introduction

The Follow-up to the 2010 Audit of Internet and Email Usage Policies and Procedures was included in the Auditor General's Audit Plan.

The key findings of the original 2010 audit included:

- Corporate email and Internet policies at the City of Ottawa are in accordance with industry practices but some areas require further attention.
- The audit recommends that the City review the existing three month retention period for Corporate emails.
- Currently, email records are retained for only three months and the audit recommends that the retention period be reviewed to ensure it is sufficient for both legal and IT requirements. In addition, there may be no City record of information exchanged by PIN to PIN (personal identification number) handheld devices.

Summary of the Level of Completion

The table below outlines our assessment of the level of completion of each recommendation as of December 2012. It also outlines management's assessment of the level of completion of each recommendation as of January 2013.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	-	-	-
Partially Complete	50 – 74	-	-	-
Substantially Complete	75 – 99	3	1	33%
Complete	100	1, 2	2	67%
total			3	100%

Conclusion

The City addressed the recommendations of the audit and has essentially completed their implementation.

Acknowledgement

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.

RÉSUMÉ

Introduction

Le Suivi de la vérification des politiques et procédures concernant l'utilisation des services d'Internet et du courriel de 2010 était prévu dans le Plan de vérification du vérificateur général.

Les principales constatations de la vérification de 2010 sont les suivantes :

- Les politiques concernant l'utilisation des services de courriel et d'Internet à la Ville d'Ottawa sont conformes aux pratiques en vigueur dans ce secteur, mais certains aspects nécessitent une attention particulière.
- La vérification recommande que la Ville révise la durée de conservation actuelles de trois mois pour les courriels de la Ville.
- À l'heure actuelle, les dossiers du système de courriel ne sont conservés que pendant trois mois et le rapport de vérification recommande que la durée de conservation soit révisée pour assurer quelle suffise aux exigences législatives et des TI. De plus, la Ville n'a peut-être aucun relevé de l'information échangée au moyen d'appareils portables NIP à NIP (numéro d'identification personnel).

Sommaire du degré d'achèvement

Le tableau ci-dessous présente notre évaluation du degré d'achèvement de chaque recommandation au mois de décembre 2012. Celui-ci présente également l'évaluation de la direction concernant le degré de réalisation de chaque recommandation au mois de janvier 2013 :

Catégorie	Pourcentage complété	Recommandations	Nombre de recommandations	Pourcentage du total des recommandations
Peu ou pas de mesures prises	0 – 24	-	-	-
Action amorcée	25 – 49	-	-	-
Complétée en partie	50 – 74	-	-	-
Pratiquement complétée	75 – 99	3	1	33 %
Complétée	100	1, 2	2	67 %
total			3	100 %

Conclusion

La Ville a traité les recommandations de la vérification et les a en grande partie mis en œuvre.

Remerciements

Nous tenons à remercier la direction pour la coopération et l'assistance accordées à l'équipe de vérification.

1 INTRODUCTION

The Follow-up to the 2010 Audit of Internet and Email Usage Policies and Procedures was included in the Auditor General's Audit Plan.

The key findings of the original 2010 audit included:

- Corporate email and Internet policies at the City of Ottawa are in accordance with industry practices but some areas require further attention.
- The audit recommends that the City review the existing three month retention period for Corporate emails.
- Currently, email records are retained for only three months and the audit recommends that the retention period be reviewed to ensure it is sufficient for both legal and IT requirements. In addition, there may be no City record of information exchanged by PIN to PIN (personal identification number) handheld devices.

2 FINDINGS OF THE ORIGINAL 2010 AUDIT

2.1 Responsible Computing Policy

Currently, the City of Ottawa Responsible Computing Policy (RCP) is up to date, with the last review having taken place on January 6, 2010. The three appendices to the RCP, (Website Blocking Standard; Electronic Messaging Guidelines; and, Data Logging Standard) focus on specific aspects of Internet and email usage and management. The RCP is a governance document and its requirements are mandatory for all information technology users of the City of Ottawa.

The RCP is in conformity with industry practices for this type of document. The level of compliance to ISO 27002:2005 may vary depending on an organization's needs, and the requirements and scope of the RCP are adequate to suit the City of Ottawa's needs. The City should however clarify what kind of non-business use of these resources it will permit.

The use of computing resources has to be specified as being for business purposes only, or for personal use purposes (as specified in point 2.3 of the RCP) only if there are no productivity impacts. As an example, we may cite restriction of the use of personal email or newsgroups to only lunchtime or outside of working hours.

Currently, "incidental" use is permitted, but this is open to wide interpretation. All City of Ottawa users are required to comply with the RCP and the IM/IT Department has control of the information technology resources that the City offers to its employees.

The Responsible Computing Policy is the main document that guides the use of information technology resources at the City of Ottawa. Other documents, such as the IM/IT Security Policy and Security Standards, are more specific to certain aspects, such as adherence to security controls and their application by IT staff, and the technology solutions that are used by the City in general.

Generally, the City of Ottawa Internet and email usage policies, which are within the scope of this analysis, are in conformity with ISO 27002:2005 specifications and controls.

At the present time, the use of a risk assessment methodology is mentioned in the Responsible Computing Policy, IM/IT Security and the Security Standards. Risk assessment methodologies are: OCTAVE, MEHARI, ISO 27005, etc. We accepted that the City developed its own practice and the City should ensure that any change, implementation, development and new process is analysed for the security risks it may pose to the whole infrastructure and to the existing processes, as well as to the information processed by the City's information resources.

The ITS Department utilizes a modified Royal Canadian Mounted Police (RCMP) risk assessment process to evaluate all technology projects. This high-level risk assessment process provides for the ability to highlight those projects that may be of a higher risk, which in turn allows the Department to focus resources to mitigate the associated risks. In 2010, the ITS Department conducted five of these high level assessments.

2.2 Records Management Policy and Record Retention and Disposition Schedule

The Records Management Policy (RMP) was updated on April 6, 2010. It is based on CAN/CGSB 72.34-2005 "Electronic Documents as Documentary Evidence" and complies with City regulations and by-laws, and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The Record Retention and Disposition Schedule is an internal document that defines retention terms for corporate records.

Presently, the email system is not an official business records repository according to Records Management Policy, (p. 12, "Policy Requirements" section) and as such, email correspondence is deleted periodically. In general, records of email traffic are only maintained for a three month period. In some cases, emails that have been deleted cannot be restored, even within this three month period. Email traffic logs are retained for 12 months; email content within an individual's mailbox is retained for three months.

Email traffic logs, according to the evidence provided by the City, do not contain any email body or content record whatsoever. As mentioned further, only the email messages (as an equivalent of paper mail) can be considered records. These records have to be archived applying the same security controls as the regular mail.

As the traffic logs cannot be considered email records, the retention period stays at three months. Another aspect is deleted email. It should be moved to the deleted email folder and not permanently deleted. These requirements arise from the City's obligations as a juridical entity that respects the Municipal Freedom of Information and Protection of Privacy Act (as noted in the Records Management Policy) and Records Retention and Disposition By-law.

Only separate email messages could be considered official records according to the conditions specified in the Records Management Policy.

Email traffic logs cannot be considered full records. As stated previously, emails (separate email messages) only can be considered as records. According to the Records Retention and Disposition Schedule the general files of the majority of the subject contents (Column 2) have a retention period of three years and an absolute majority has a retention period of at least 1 year. This means, in our understanding, that the business related email correspondence, according to RCP and RCP Appendix B 'Electronic messaging guidelines' has to comply with the Records Retention and Disposition By-law.

A review of the retention schedule is recommended in order to ensure a longer time span for the retention of the City's email correspondence. The implications of a shorter retention period are multiple; the most evident being the deletion of activity evidence and documents that might have been transmitted by email. Considering that legal, financial, accounting and other types of documents might be transmitted by email, the Records Retention and Disposition Schedule could apply, and those specified retention periods would have to be respected. Where legal, financial, accounting and other types of documents are transmitted by email, the Records Retention and Disposition Schedule does apply. In order to preserve an activity trail of email correspondence, a retention period of three to five years is recommended, in conformity with the Records Retention and Disposition Schedule for written correspondence. An email archiving tool might be considered in order to facilitate records management.

This illustrates that the email may and in many cases is used for sending all kinds of sensitive information that falls under one or more categories of the Records Retention and Disposition Schedule. Thus, in order to ensure the application of the said Schedule and By-law that enables it, the emails have to be preserved as corporate correspondence, even deleted email. By doing this, the IT/IM Department will comply with City's own By-law.

There is no commonly accepted standard or law that indicates a specific term for email retention, however given the difficulty of filtering official and unofficial email, it is a common industry practice to preserve whole email correspondence in order to ensure appropriate corporate records management. If the IT/IM Department is able to propose a way to filter business and non-business email with

a comfortable level of assurance, then it could be discussed internally and proposed to senior management for approval and eventually accepted into production.

2.3 Information Management/Information Technology Security Policy

The Information Management/Information Technology Security Policy is a document produced to ensure the protection of information transmitted over the City network. It is intended for those users that are responsible for the provision and administration of information technology services. General users are not subject to the IT/IM Security Policy as it covers risk management safeguards and defines elements of information security that are to be ensured for data on the City's network.

The current RCP notion for IT assets covers hardware equipment only. Recognizing software as an IT asset will ensure that it is managed and protected in the same way as hardware.

Currently, some information transmitted on corporate handheld and mobile devices does not go through the City network system. (PIN to PIN and SMS messages are not logged on the corporate network as per the Responsible Computing Policy.) If corporate records are sent PIN to PIN, there may be no record of this data on the City network. Corporate records should not therefore be communicated PIN to PIN. All emails and documents transmitted on laptops, tough books, and smart phones go through the City's email network. Voice calls made through corporate handheld and mobile devices have key transaction artefacts logged such as the number and time.

For those using handhelds and mobile devices, email correspondence leaves the corporate network (the telephone provider is not part of the City network). This means that it is not under the full control of the IT/IM Department. Thus, a specific section or policy intended for those who carry corporate handhelds may need to be put in place. By doing this, the City ensures that handheld and smartphone users are aware that those devices hold sensitive information and due care and due diligence should apply.

Also, the increased use of mobile devices creates unique security risks, including the risk of unauthorized access to data. There is also greater risk that information of a private nature may be accessed by unauthorized persons.

The most obvious example of a unique security risk is the loss of an unlocked handheld. This does not mean that the IT/IM Department creates the risk, but that the enacting of a policy requiring the handhelds to be locked in all times could be necessary.

Management indicates that the Responsible Computing Policy and the City of Ottawa's Code of Conduct govern the use of these mobile devices. Handheld and

mobile devices are configured in the same manner as City laptops. This configuration includes: encryption of data at arrest and in transmission, password protection of the device, lock down to prohibit the installation of unauthorized software, and remote wiping for lost/stolen devices.

The use of staff's own personal mobile devices while in the workplace is also an emerging issue. We recommend that management proactively deal with the growing use of staff's own personal mobile devices while at work by establishing and enforcing an appropriate policy.

2.4 City of Ottawa Information Management/Information Technology Security Standards v1.10

The City of Ottawa Information Management/Information Technology Security Standards v1.10 is intended to clarify aspects of the IM/IT Security Policy, and to detail and complete the policy specifications.

Requirements and statements contained within the documents that were reviewed are of no use if not reinforced and user compliance monitored. The purpose of policies is to protect the City's IT network as a vital service, and to educate the users in order to optimize the use of equipment and services over the network. In order to ensure that policies are adhered to, users should be notified any time there are monitoring and control tools filtering and analyzing the use of the City's resources. Ideally, permanent monitoring should be in place, and management should decide the consequences resulting from policy violation.

This relates to the fact that as per discussions held with management, it was stated that filtering and protection equipment is used mainly in reaction to incidents and violations. In order to ensure the application of security controls and best practices, permanent monitoring is an obvious option that will permit the identification of behaviour or incident patterns in a timely manner.

It should be mentioned that Internet and email monitoring tools are currently used for incident monitoring and not for operational usage monitoring. Operational monitoring of user activity would provide a better understanding of Internet and email usage on the City network, but that will necessitate a change of view on monitoring. The City could decide on this change of principle and act accordingly to implement it.

Operational usage monitoring is strongly related to permanent monitoring and means allowing resources for overseeing user activity on a permanent basis, not only in case of incidents. The 'operational usage monitoring' will permit a better security position for the City and will ensure security controls contained in the RCP and its appendices, standards and procedures are applied and respected in all times.

Currently, the IM/IT Security standards have not been updated or reviewed since November 3, 2008. The IM/IT Security Policy has not been updated since January 25, 2007. Security standards, as stated in Section 3.3, are to be developed as the City's IT environment and network change. In order to document these changes, and offer a security view on the technologies and processes, the standards need to be updated on a regular basis.

The Security Policy should be reviewed at least on a yearly basis, and should take into account the development and evolution of the IT function. If no changes are needed, a review and re-approval process should take place and the policy should be re-issued to the user community as a reminder of the City's efforts in that regard.

Improved monitoring and control tools usage would mean a regular analysis of user activity in order to ensure compliance to the RCP and other security policy documents at the City. No specific action and end state can be proposed here because it would mean a more thorough evaluation. Otherwise, tools that perform monitoring and control exist at the City (e.g., Websense, Promodag) and others may be implemented depending on management's decisions to improve the City's security position. Optimised use of existing tools, their update, operational monitoring (as stated earlier) may be considered before changing the existing architecture.

During the course of the audit in December 2010, ITS put in place an intrusion prevention and security information and event management service. ITS has contracted a Canadian based managed security service provider that provides 24/7 monitoring of our web-facing services (Ottawa.ca, etc.) and other critical components of the network. During the course of the audit, we had indicated to ITS that monitoring and control tools usage over the City's network should be improved. In our opinion, this new contract helps to address this issue.

3 STATUS OF IMPLEMENTATION OF 2010 AUDIT RECOMMENDATIONS

2010 Recommendation 1

That the City review the existing three month retention period for emails, including deleted emails, to ensure it is sufficient. Both legal and IT requirements should be considered.

2010 Management Response

Management agrees with this recommendation.

Management will review the existing three month retention period for emails considering both legal and IT requirements, and will provide a report on this subject to the IT Sub-Committee by the end of Q4 2011.

Management Representation of the Status of Implementation of Recommendation 1 as of July 3, 2012

The City Clerk and Solicitor, the Office of the Auditor General and the Director of Information Technology Services and Chief Information Officer met in June of 2011 to review the existing three month retention period for emails. At that time, it was confirmed that there was no Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), labour relations or other legal or corporate requirements for extending the e-mail archiving period from 90-days to two years. This information was reported to, and received by, the IT Sub-Committee (August 22, 2011), the Finance and Economic Development Committee (FEDC) (September 6, 2011) and City Council (September 14, 2011) via report ACS2011-COS-ITS-0005.

Management: % complete ***100%***

OAG's Follow-up Audit Findings regarding Recommendation 1

We have reviewed the IT Sub-Committee report: ACS2011-COS-ITS-0005 which concluded that: "Given the consensus that there is no corporate requirement, as well as that the cost to implement a two year archive is high (estimated at between $250K and $1M), no changes to the current email management practices and associated policies are proposed."

At their meeting of August 22, 2011, the IT Sub-Committee recommended that the FEDC recommend that Council receive the report for information.

The FEDC received the report.

As per the minutes from the FEDC meeting of September 6, 2011, FEDC recommended that Council receive the report for information.

And, as per the minutes from the September 14th City Council meeting, the report was received for information.

OAG: % complete ***100%***

2010 Recommendation 2

That the City formalize and include in the Responsible Computing Policy an extended notion of IT assets to include software.

2010 Management Response

Management agrees with this recommendation.

The Responsible Computing Policy will be updated to include the addition of software as a City of Ottawa information technology asset by the end of Q3 2011.

Management Representation of the Status of Implementation of Recommendation 2 as of July 3, 2012

The Responsible Computing Policy was revised in August 2011 to include software as an asset.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 2

The Responsible Computing Policy revised in August 2011 was reviewed and the notion of IT assets includes software.

OAG: % complete 100%

2010 Recommendation 3

That the City keep Security Standards up to date and review the policies at least on a yearly basis.

2010 Management Response

Management agrees with this recommendation.

A review of the Security Standards will be incorporated into the ITS Department annual operational plans, and an initial review will be undertaken by the end of Q2 2012.

Management Representation of the Status of Implementation of Recommendation 3 as of July 3, 2012

A review of the security standards (IM/IT Security Standards) was undertaken in 2012 and as a result, the ITS department has replaced those standards with the Information Systems Security Policy (ISSP). The ITS department will conduct an annual review of this policy.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 3

The security standard was replaced by the two policies. The first policy is the Information Security Policy (ISP) effective on August 29, 2011; the second is the Information Systems Security Policy (ISSP), effective on September 1, 2012.

The City has a Corporate Administrative Policy Handbook (April 2010) that presents the City corporate governance principle toward policies. The Handbook clearly determines that policies are reviewed based upon emerging needs or according to schedule, every three years.

The City ITS management recognized that it is important to stay current with technology and plans on reviewing those policies annually. It is planned to capture this annual commitment in a specific work plan in 2013.

This recommendation is essentially completed and is to be implemented; however, it is not fully implemented until the annual review is added to the 2013 work plan.

OAG: % complete ***90%***

Management Representation of Status of Implementation of Recommendation 3 as of January 31, 2013

Management agrees with the follow-up audit findings.

The annual review of the Information Security Policy (ISP) and Information Systems Security Policy (ISSP) will be added to the ITS 2013 departmental work plan and is scheduled to be completed by Q4 2013.

Management: % complete ***90%***

4 SUMMARY OF THE LEVEL OF COMPLETION

The table below outlines our assessment of the level of completion of each recommendation as of December 2012. It also outlines management's assessment of the level of completion of each recommendation as of January 2013.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	-	-	-
Partially Complete	50 – 74	-	-	-
Substantially Complete	75 – 99	3	1	33%
Complete	100	1, 2	2	67%
total			3	100%

5 CONCLUSION

The City addressed the recommendations of the audit and has essentially completed their implementation.

6 ACKNOWLEDGEMENT

We wish to express our appreciation for the cooperation and assistance afforded the audit team by management.