Office of the Auditor General / Bureau du vérificateur général

FOLLOW-UP TO THE 2005 AUDIT OF INTERNET USAGE AND CONTROLS

2010

SUIVI DE LA VÉRIFICATION DE L'UTILISATION ET DE CONTRÔLES D'INTERNET DE 2005

Table of Contents

EXECUTIVE SUMMARY

Introduction

The Follow-up to the 2005 Audit of Internet Usage and Controls was included in the Auditor General's Audit Plan.

The key findings of the original 2005 audit included:

- Updating the City's anti-virus software;
- Improving log management practices to allow for detection of malicious activity and to track trends; and,
- Prohibiting the installation of software not officially sanctioned.

Summary of the Level of Completion

1. The table below outlines our assessment of the level of completion of each recommendation as of Spring 2010.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	7b, 7f	2	5%
Partially Complete	50 – 74	18a, 18b, 18c, 18d	4	10%
Substantially Complete	75 – 99	7c, 7g, 12, 14, 15, 21a*, 21b*, 21c*	8	19%
Complete	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 16, 17a, 17b, 17c,19a*, 19b*, 20*	27	66%
TOTAL			41	100%

2. The table below outlines management's assessment of the level of completion of each recommendation as of Summer 2010 in response to the OAG's assessment. These assessments have not been audited.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	7b, 7f	2	5%
Partially Complete	50 – 74	-	-	-
Substantially Complete	75 – 99	7c, 7g, 12, 21a*, 21b*, 21c*	6	15%
Complete	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 14, 15, 16, 17a, 17b, 17c, 18a, 18b, 18c, 18d, 19a*, 19b*, 20*	33	80%
TOTAL			41	100%

*Confidential recommendations are omitted from this report as they contain information that could compromise the City's information technology security.

Conclusion

Most of the recommendations from the 2005 Audit of Internet Usage and Controls have been implemented by the Information Technology Services (ITS) Department. The main issues identified relate to monitoring of staff Internet and e-mail activity. In 2009, two Cisco PIX firewalls were nearing the end of their useful life and manufacturer's support and have been replaced by newer ASA firewalls in 2010. This will offer increased stability and manufacturer support in case of incidents. There was no Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) on the network at the time we conducted this follow-up audit, but the ITS Department is in the process of implementing such devices. These efforts align with the implementation of the Payment Card Industry (PCI) requirements which the City of Ottawa is subject to.

The requested Websense reports containing City staff's Internet use could not be provided due to technical difficulties. The ITS Department is deploying its efforts to provide these documents and these will be reviewed. As is, the City of Ottawa internal network generally meets industry best practices for secure architecture and use of appropriate protection technologies. The Security Information and Event Management (SIEM) project will add strength from a security standpoint to the City's network, considering the IDS/IPS devices are part of the implementation.

There is no evidence that sensitive information is being encrypted on the City network. No document has been provided indicating information classification and/or guidelines for its handling. Implementation of PCI requirements will require such tools; as a minimum for banking and personal data that is transmitted over the City network. Once implementation of current PCI requirements is achieved, these deficiencies will probably be rectified.

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 de l'utilisation et de contrôles d'Internet de 2005 était prévu dans le Plan de vérification du vérificateur général.

Les principales constatations de la vérification de 2005 sont les suivantes :

- la mise à jour du logiciel antivirus de la Ville;
- l'amélioration des pratiques de gestion du journal pouvant permettre la détection d'activités malicieuses ou assurer le suivi des tendances;
- l'interdiction d'installer des logiciels sans d'abord obtenir l'approbation officielle.

Sommaire du degré d'achèvement

1. Le tableau ci-dessous présente notre évaluation du degré d'achèvement de chaque recommandation au printemps 2010 :

CATÉGORIE	POURCENTAGE COMPLÉTÉ	RECOMMANDATIONS	NOMBRE DE RECOMMANDATIONS	POURCENTAGE DU TOTAL DES RECOMMANDATIONS
PEU OU PAS DE MESURES PRISES	0 – 24	-	-	-
ACTION AMORCÉE	25 – 49	7b, 7f	2	5 %
COMPLÉTÉE EN PARTIE	50 – 74	18a, 18b, 18c, 18d	4	10 %
PRATIQUEMENT COMPLÉTÉE	75 – 99	7c, 7g, 12, 14, 15, 21a*, 21b*, 21c*	8	19 %
COMPLÉTÉE	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 16, 17a, 17b, 17c,19a*, 19b*, 20*	27	66 %
TOTAL			41	100 %

2. Le tableau ci-dessous présente l'évaluation de la direction concernant le degré de réalisation de chaque recommandation à l'été 2010 en réponse à l'évaluation du Bureau du vérificateur général. Ces évaluations n'ont pas fait l'objet d'une vérification.

Catégorie	Pourcentage complété	Recommandations	Nombre de recommandations	Pourcentage du total des recommandations
Peu ou pas de mesures prises	0 – 24	-	-	-
Action amorcée	25 – 49	7b, 7f	2	5 %
Complétée en partie	50 – 74	-	-	-
Pratiquement complétée	75 – 99	7c, 7g, 12, 21a*, 21b*, 21c*	6	15 %
Complétée	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 14, 15, 16, 17a, 17b, 17c, 18a, 18b, 18c, 18d, 19a*, 19b*, 20*	33	80 %
TOTAL			41	100 %

*Les recommandations confidentielles ne figurent pas dans ce rapport; elles contiennent en effet des renseignements qui pourraient compromettre la sécurité de la technologie de l'information de la Ville.

Conclusion

Le Service de technologie de l'information (STI) a mis en œuvre la plupart des recommandations de la vérification de 2005 de l'utilisation et de contrôles d'Internet. Les principales problèmes cernés sont liées au contrôle de l'usage d'Internet par le personnel ainsi que des activités relatives aux courriels. Deux pare-feux Cisco PIX, qui avaient atteint la fin de leur cycle de vie et de soutien en 2009, ont été remplacés par des pare-feux ASA plus récents en 2010, ce qui entraînera une stabilité accrue et un soutien du fabricant en cas d'incidents. Aucun système de détection d'intrusion ni aucune vérification du rendement de l'installation n'étaient installés sur le réseau au moment de la vérification, mais le STI procède actuellement à l'installation de tels dispositifs. Ces efforts sont conformes à la mise en œuvre des exigences relatives aux normes de sécurité du secteur des cartes de paiement « PCI » auxquelles la Ville est soumise.

Les rapports Websense requis faisant part de l'utilisation de l'Internet par le personnel municipal n'ont pas pu être présentés en raison de difficultés techniques. Le STI déploie tous ses efforts afin de fournir ces documents qui seront examinés. Tel qu'il est, le réseau interne de la Ville d'Ottawa respecte de façon générale les meilleures pratiques de l'industrie en ce qui a trait à l'architecture sécuritaire et à l'utilisation appropriée de technologies de protection. Pour ce qui est de la sécurité, le projet SIEM renforcera de façon constante le réseau de la Ville, si l'on considère que les dispositifs de système de détection d'intrusion et de vérification du rendement de l'installation font partie de la mise en œuvre.

Rien ne prouve que des renseignements sensibles sont encodés sur le réseau de la Ville. Aucun document n'a été fourni précisant la classification des renseignements et/ou les règles concernant leur gestion. La mise en œuvre des exigences du PCI requerra de tels outils au moins pour les données bancaires et personnelles qui circulent sur le réseau de la Ville. Une fois la mise en œuvre des exigences du PCI actuelles, ces lacunes seront probablement corrigées.

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 2005 Audit of Internet Usage and Controls was included in the Auditor General's Audit Plan.

Specific Internet security recommendations in the audit include:

- Updating the City's anti-virus software;
- Improving log management practices to allow for detection of malicious activity and to track trends; and,
- Prohibiting the installation of software not officially sanctioned.

2 KEY FINDINGS OF THE ORIGINAL 2005 AUDIT OF INTERNET CONTROL AND USAGE

1. The e-mail controls to safeguard system/information confidentiality, integrity and availability worked as expected. Specifically, we found that the security controls surrounding the e-mail isolation of dangerous attachments were successful. Even though knowledgeable users were found to be able to bypass file type blocking controls, they were not able to bypass anti-virus controls and the nine anti-virus engines blocked malicious file content.
2. Although, we found that Library and Employment Centre Public Desktop Lockdown could be greatly improved from providing an automated Windows XP patching, and the latest Symantec Antivirus version.
3. We determined that the implementation of the anti-spam firewall in January 2004 had greatly reduced the amount of SPAM e-mail that City staff must process and, reduced the possibility of the SPAM setting off a malicious software infestation, and reduced the e-mail delivery system resource requirements.

3 STATUS OF IMPLEMENTATION OF 2005 AUDIT RECOMMENDATIONS

2005 Recommendation 1

That Information Technology Services investigate the tools used to perform blocking by file type to enable this feature regardless of extension.

2005 Recommendation 2

That Information Technology Services deploy the latest Symantec Antivirus version.

2005 Recommendation 3

That Information Technology Services update the configuration of the Antivirus systems to include anti-virus checking on read from disk and before program execution.

2005 Management Response

Management agrees with recommendations 1, 2 and 3.

IT Services is investigating a new feature recently available for the first layer of virus-scanning protection, which permits blocking of file types regardless of the extension used. Testing to ensure there is no negative impact on e-mail delivery services will occur in Q1 2006.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

Management Representation of the Status of Implementation of Recommendation 1, 2 and 3 as of December 31, 2008

Implementation of these recommendations is 100% complete.

Management: % complete (1)	***100%***
Management: % complete (2)	***100%***
Management: % complete (3)	***100%***

OAG's Follow-up Audit Findings regarding Recommendation 1, 2 and 3

Implementation of recommendations 1, 2 and 3 is 100% complete. For recommendation 1, the ITS Department provided evidence of the implementation of the "blocking by file type" functionality in their environment.

Recommendation 2 was fulfilled by the implementation and use on the standard corporate image of a fully vendor supported version of Symantec Anti-Virus.

Recommendation 3 was implemented successfully by the ITS Department and evidence of the standard Antivirus engine configuration was provided.

OAG: % complete (1) ***100%***

OAG: % complete (2) ***100%***

OAG: % complete (3) ***100%***

2005 Recommendation 4

That Information Technology Services:

a) Review the level of awareness of the SPAM e-mailbox and increase visibility if warranted; and

b) Continue monitoring of the effectiveness of the current SPAM filtering tool.

2005 Management Response

Management agrees with these recommendations.

The spam@ottawa.ca mailbox continues to be part of IT Services' ongoing security awareness program. Over 1,000 e-mails received by City staff from external sources are submitted monthly to the SPAM mailbox for review. In addition, four City Brief articles were published in 2005 on the topic of SPAM, each including a reminder about the availability of the SPAM mailbox. IT Services will continue to remind staff of the SPAM e-mailbox regularly.

Upgrades to the SPAM filtering service are implemented by IT Services when available from the vendor, to ensure continued effectiveness of the service. As noted in the report, monitoring of the SPAM filtering service is performed daily, and reviewed monthly by IT Services.

October data from MessageLabs indicated that 65% of all e-mail worldwide was identified as SPAM. Of the 50,000 e-mails received from external sources daily to the City's 9,000 e-mail users, slightly over 50% is identified as SPAM and immediately rejected. Roughly 0.5% of these e-mails are SPAM that is not identified or rejected, and successfully reaches a City recipient – 250 e-mails per day for the entire City. Users are encouraged to forward SPAM messages to IT Services to assist in increasing the effectiveness of the SPAM filtering service.

Management Representation of the Status of Implementation of Recommendation 4 as of December 31, 2008

Implementation of this recommendation is 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 4

Implementation of recommendation 4 is 100% complete. The City's ITS Department provided the auditors with the requested evidence of implementation such as regular e-mails that increase the visibility of the "SPAM mailbox" and the job description of the Network Analyst responsible for monitoring and ensuring the functionality of the SPAM filtering tool. The ITS Department also provided a monthly report produced to monitor the SPAM filtering services.

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

2005 Recommendation 5

That Information Technology Services:

a) Tighten the Websense service implementation to reduce possibility of service bypass.

b) Review some level of Library filtering to reduce the risk, such as a limited number of isolated general use systems for unfiltered web access. If this cannot be completed to an appropriate level, then Information Technology Services should consider separating the Ottawa Public Library from the City's system.

2005 Management Response

a) Management agrees with this recommendation.

In 2005, prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. At the time of writing this response (November 2005), an extensive range of additional Websense filtering features is now in place.

The audit findings identified one small site (the Don Gamble Community Centre) that allowed City of Ottawa staff unfiltered access to the Internet. This was a subnet routing issue that misidentified these four City staff to Websense as Library staff workstations, which are unfiltered (see below). IT Services has corrected this routing issue.

b) Unfiltered Internet access is provided to Ottawa Public Library (OPL) staff for reasons of intellectual freedom. This is as a result of a Library Board directive and therefore is a governance issue with the Library Board and outside the jurisdiction of the IT Services Branch.

c) Since 2001, a considerable amount of effort from IT Services has been directed to manage the risk of this configuration. For example, Library workstations are on separate network segments that make it easy to isolate viruses, worms and spyware in the event of a malicious code outbreak. On the advice of IT Services staff, Library Management agreed, in October 2005, to allow IT Services to protect their workstations from Internet-borne malicious code. The workstations used by

Library staff do not allow staff to visit malicious websites, however they remain completely unfiltered for all other website content.

Given the OPL is governed by the Library Board, it may not be possible to influence the Board to reverse the decision to allow unlimited access to Internet sites based on the principle of intellectual freedom. Therefore if filtering cannot be implemented to a reasonable level, ITS Branch agrees with the recommendation that consideration should be given to separate the Ottawa Public Library from the City's system. This would be a significant undertaking as the Ottawa Public Library (OPL) is spread across 33 different sites throughout the City. Furthermore, separating the Ottawa Public Library from the City of Ottawa network would incur significant additional costs, due to the sharing of business applications and IT Services resources between OPL and the City.

It is estimated that the cost to separate the Ottawa Public Library from the City's network would be $30,000 of one time capital funding and $150,000 of annual operating costs, including the funding of 1 additional FTE (or equivalent). A budget pressure will be identified for the 2007 budget.

Management Representation of the Status of Implementation of Recommendation 5 as of December 31, 2008

a) Implementation of this recommendation is 100% complete.

b) Implementation of this recommendation is 100% complete. The Ottawa Public Library Board approved a new restricted XP desktop image in June 2005, which controls access to instant messaging programs. In addition, the Library Board further supported the recommendation to begin filtering malicious Internet traffic later that year. With the implementation of a Websense Security premium group and XP desktop controls, IT Services considers the risk to the City network sufficiently mitigated.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 5

a) Implementation of recommendation 5a) is 100% complete. The ITS Department provided the auditors with the requested evidence of implementation i.e., the updated Websense architecture at the City. The configuration presented reflects the standard implementation recommended by the equipment manufacturer. The Library traffic is filtered through the Websense system on a policy based principle. The Library Websense policy is less restrictive than for other City users. ITS Department Management explained that this is in accordance with the Library Board by-laws that permit a broader access than for other City employees.

b) At the current time, the implementation of this recommendation is 100% complete. Evidence of the actions taken to prevent access to malicious sites has been provided in the form of the Websense Policy export. However, the unfiltered access for Library staff is still available to some site categories that might be considered of restricted access and are not available to other City employees. According to the ITS Department, the general use systems are restricted and the permitted access is in conformity with Library Board by-laws.

The Websense Web Filter is subject to the second part of the Internet and e-mail usage follow-up audit. The use of the Websense filtering tool as well as the functionality and performance evaluations will be presented in a second report.

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

2005 Recommendation 6

That Information Technology Services:

a) Deploy the latest Symantec Antivirus version; and

b) Update the configuration of the Anti-Virus systems includes anti-virus checking before file read and before program execution.

2005 Management Response

Management agrees with this recommendation.

IT Services considers that the risk of using the current version of Symantec Antivirus (7.61) is mitigated as three additional layers of anti-virus and malicious file protection also safeguard the City network, and Symantec continues to issue updated virus signature files per the support agreement up to January 31, 2006.

It is not uncommon for an organization of the size of the City of Ottawa to delay or skip version upgrades of software products. Upgrades are done either because the new functionality offered is needed by the City and is supported by a business case for the upgrade, or because the product is no longer supported by the vendor. IT Services has evaluated the additional features and business case for each new version as it is released. In fact, the City partnered with Symantec in Q1 2005 to beta-test version 10, as this is the first version to add features to safeguard against the current threat from spyware. Following this evaluation, Symantec recommended in late Q3 2005 that the City begin a managed upgrade directly from version 7.61 to Symantec Antivirus version 10.

IT Services initiated the upgrade to Symantec Antivirus 10 in Q4 2005, to be completed by January 31, 2006. This upgrade includes an assessment of the productivity impact of including anti-virus checking on read from disk and before program execution.

Management Representation of the Status of Implementation of Recommendation 6 as of December 31, 2008

Implementation of these recommendations is 100% complete.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 6

Implementation of this recommendation is 100% complete. The City has deployed a supported version of the Symantec Antivirus 10.1, although not the latest, which is Symantec Endpoint Protection 11.0. A supported version of a product provides assurance of the manufacturer's assistance in case of problems. The ITS Department provided evidence of enabling of the "check before file read and before file execution" functionality.

OAG: % complete 100%

2005 Recommendation 7

That Information Technology Services:

a) Review logging and monitoring processes and systems for effective operational system health and policy enforcement monitoring;

b) Identify log events that require "real time" detection and alerting and implement appropriate processes;

c) Review all security devices to ensure appropriate logging coverage;

d) Ensure all device clocks are centrally synchronized for effective event correlation;

e) Review regulatory and City policy requirements for an appropriate logging data retention period;

f) Consider feeding log and monitoring data into a Security Information Management (SIM) tool for automated event analysis and correlation, to better provide a near real time City security posture;

g) Ensure all devices are logging operational health and security events as a minimum; and

h) Enable system logging on all devices.

2005 Management Response

Management does not completely agree with these recommendations.

Industry best practices do not support full logging on all devices at all times due to the high cost. IT Services implements additional logging and alerting on a selective basis, such as with certain high-risk devices or where there is a concern with a particular device.

As part of the Enterprise Security Review project initiated in Q1 2005, IT Services has contracted a third party security company to perform a detailed review of logging and monitoring processes and systems, including an assessment of the cost impact of these recommendations. The review will be completed in Q1 2006. If additional logging is required, a budget pressure will be identified in the 2007 budget. IT Services has implemented alerting for device failure on all servers and network devices.

IT Services has updated all firewalls to receive a synchronized time from NRC.

A review of regulatory and City policy requirements for logging data will be completed in Q2 2006, following the detailed review of logging and monitoring processes and systems in Q1 2006. Log data will be retained in accordance with the City's Records Management Policy and By-Law.

The need for additional logging and Security Information Management (SIM) tool will be assessed in Q2 2006 and if required a budget pressure will be identified in the 2007 budget. Additional logging is estimated to cost between $75,000 - $150,000. To purchase and implement a SIM is $150,000, with ongoing operating costs in excess of $200,000 per year. Ongoing FTE (or equivalent) requirements are unknown at this time.

Management Representation of the Status of Implementation of Recommendation 7 as of December 31, 2008

Implementation of recommendations 7a), c), d), e) and g) are 100% complete.

Implementation of recommendations 7b) and f) are 20% complete. A project has been launched to implement a security event management and intrusion detection system. A Request for Proposal is scheduled for release on January 19, 2009, bid evaluations will be completed by March 13, 2009, and a contract award will follow by March 27, 2009.

Implementation of recommendation 7h) is 100% complete. This item was discussed at CAWG on March 6, 2007 and was approved by Council on May 9, 2007. As a result of discussions at CAWG and subsequent discussions with the Auditor General, the following work plan was deemed acceptable and has now been completed:

2007:

Q3-Q4: Procure a system-logging server to act as the repository for log data.

Q4: Adjust levels of logging on network devices and begin feeding log data to the system-logging server.

2008:

Q1-Q2: Evaluate and procure available log auditing and analysis tools. Both in-house and outsourced solutions to be evaluated.

Q2-Q3: Develop formal log analysis and auditing procedures.

Q4: Implement formal log analysis and auditing procedures.

Management: % complete (a)	***100%***
Management: % complete (b)	***20%***
Management: % complete (c)	***100%***
Management: % complete (d)	***100%***
Management: % complete (e)	***100%***
Management: % complete (f)	***20%***
Management: % complete (g)	***100%***
Management: % complete (h)	***100%***

OAG's Follow-up Audit Findings regarding Recommendation 7

a) Implementation of recommendation 7a) is 100% complete. The ITS Department logs the City security devices health status as requested and monitors the effective operational system health of these devices.

b) Implementation of recommendation 7b) is 25% complete. The existing systems are sending warnings based on predefined rules. According to an independent evaluation of the logging practices at the City, the ITS Department's actions are mostly reactive and logs are reviewed mainly when problems occur. Furthermore, according to the independent assessment, the logging practices on the Cisco PIX security devices provide minimal information, however, the ITS Department uses some tools to assist in the log analysis and keeps a large amount of log data for pattern analysis purposes. The upgrade from the Cisco PIX series firewalls to Cisco ASA will keep the same functionality in regards to logging, unless CSM version 4.0 is used for log analysis. Currently, the Cisco ASA firewalls are in use on the City network (per the evidence provided) and there are no logging functionality changes compared to the previous PIX implementation.

c) Implementation of recommendation 7c) is 75% complete. According to the documentation provided, the security devices logging is active but the log analysis is highly reactive. An implementation of a centralized log analysis system would highly improve the City's position in this matter. Implementation of the SIEM project, which is in its final stage, will offer the possibility to strengthen the log coverage and increase the automatic log analysis capacity of the security devices on the City network.

d) Implementation of recommendation 7d) is 100% complete. The firewall rules have been changed in order to the permit the time synchronisation, and these rules have been kept with the migration from PIX to ASA implementations.

e) Implementation of recommendation 7e) is 100% complete. The ITS Department has discussed the retention period matter and the minutes from the meeting have been provided. The current policies align with the City regulations and by-laws.

f) Implementation of recommendation 7f) is 25% complete. The ITS Department is taking the steps to choose and implement a Security Information Management tool in order to permit a better analysis and correlation of the security events. In order to improve the security position, the City plans to deploy an IDS/IPS device that will permit "real time" reaction when security breaches occur. Currently, implementation of the SIEM project is underway and is part of the overall PCI conformity effort.

g) Implementation of recommendation 7g) is 85% complete. According to the independent assessment report provided, the logging is enabled and the monitoring of the operational health and security events is ensured. However, the ITS Department keeps at minimum the logging information from the security devices and the actions to security event are mainly identified post-factum. Implementation of a centralized log analysis device and an IDS/IPS system will highly improve the City position in this matter.

h) Implementation of recommendation 7h) is 100% completed. The ITS Department provided evidence of enabled logging on firewalls, Websense Web Filters, Borderware devices, Symantec Anti Viruses, Layer 3 switches. Moreover, implementation of the SIEM project will permit a more effective log analysis and log correlation in order to assure a better security position and rapid responses to eventual threats.

OAG: % complete (a)	***100%***
OAG: % complete (b)	***25%***
OAG: % complete (c)	***75%***
OAG: % complete (d)	***100%***
OAG: % complete (e)	***100%***
OAG: % complete (f)	***25%***
OAG: % complete (g)	***85%***
OAG: % complete (h)	***100%***

Management Representation of Status of Implementation of Recommendation 7 *as of Summer 2010*

Management agrees with the OAG's follow-up audit finding.

Recommendations 7b, 7c, 7f and 7g are all being addressed by the Security Information and Event Management (SIEM) solution, which is scheduled to be fully implemented by the end of Q4 2010 as a component of the Payment Card Industry (PCI) Compliance project.

Management: % complete (a)	***100%***
Management: % complete (b)	***25%***
Management: % complete (c)	***75%***
Management: % complete (d)	***100%***
Management: % complete (e)	***100%***
Management: % complete (f)	***25%***
Management: % complete (g)	***85%***
Management: % complete (h)	***100%***

2005 Recommendation 8

That Information Technology Services:

a) Implement a more robust Change Management process/system within Corporate Services; and

b) Enforce the formal Change Management process for all changes to the firewalls and other security systems.

2005 Management Response

Management agrees with these recommendations.

The current Change Management process in place since 2001 was enhanced in Q4 2005 to encompass all IT Services divisions and the requirement to comply with the City's Records Management Policy.

The Chief Information Officer reminded all IT Services Managers and Program Managers in November 2005, of the requirement to adhere to this Change Management process. This includes the requirement to document results achieved and record these centrally using the City's Records Management framework.

Management Representation of the Status of Implementation of Recommendation 8 as of December 31, 2008

Implementation of these recommendations is 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 8

Implementation of recommendation 8 is 100% complete. The ITS Department provided evidence of the implementation of a new Change Management process, Marvel Service Management replacing Support Magic previously used. The changes to firewalls and security systems are documented and stored in a repository for this purposes.

OAG: % complete 100%

2005 Recommendation 9

That Information Technology Services ensure the policy prohibit the installation of software not officially sanctioned.

2005 Management Response

Management agrees with this recommendation.

Section 6.4 of the revised Responsible Computing Policy, approved by City Management in September 2005, states: "Users shall not install or download software, shareware, freeware or any other application program onto City-owned IT assets without the express written permission of ITS."

Management Representation of the Status of Implementation of Recommendation 9 as of December 31, 2008

Implementation of these recommendations is 100% complete.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 9

Implementation of recommendation 9 is 100% complete. Section 5.4 of the City of Ottawa Responsible Computing Policy states that installation of any non-ITS sanctioned software on the City's network is prohibited. As an enforcement mechanism, typical employee accounts are locked and the capability to install software is not permitted by default.

OAG: % complete 100 %

2005 Recommendation 10

That Information Technology Services ensure the policy prohibit the use of non-City approved computing resources for processing City data and assets.

2005 Management Response

Management does not completely agree with this recommendation.

This recommendation applies to the following two situations:

Use of non-City hardware by staff and/or consultants on the City network (e.g., laptops). Processing City data and assets using non-City hardware (e.g., home computers). IT Services concurs with the recommendation with respect to the use of non-City hardware on the City network (e.g., laptops). In section 6.3 of the revised Responsible Computing Policy, approved by City Management in September 2005, the Policy states: "Non-City hardware shall not be connected to the Corporate network without the express written consent of the ITS Branch."

IT Services does not agree with this recommendation with respect to processing City data and assets using non-City hardware (e.g., home computers). Such a restriction would prohibit the use of web-mail from a home computer, or working from home on a Word document or Excel spreadsheet. The Responsible Computing Policy clearly defines employee obligations to safeguard electronic and information records in their custody, whether being processed at a City facility or not. The City's Defence-in-Depth Strategy mitigates the risk to the corporation from malicious software brought from a non-City computing environment.

Management Representation of the Status of Implementation of Recommendation 10 as of December 31, 2008

Implementation of this recommendation is 100% complete. This item was discussed at CAWG on March 6, 2007 and was approved by Council on May 9, 2007. As a result, it was agreed that the Responsible Computing Policy would be updated to reflect prohibition of non-City assets connecting to network and the requirement to protect City information assets when accessed via web-mail.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 10

Implementation of recommendation 10 is 100% complete. Section 5.3 of the Responsible Computing Policy specifies that the users are responsible for ensuring the confidentiality, integrity and availability of City data when transmitted to non-City hardware. The City internal network is highly protected, and the access to webmail is permitted. The March 6, 2007 CAWG minutes reflect that the Office of the Auditor General agreed to consider the internal City network security measures as sufficient for the protection of the City computing resources.

OAG: % complete 100%

2005 Recommendation 11

That Information Technology Services review the retention periods for e-mail (including deleted e-mail) and compare to use of this data as corporate records and industry best practices.

2005 Management Response

Management agrees with this recommendation.

The retention period for e-mail was reviewed against federal, provincial, and municipal legislation prior to approval of the Records Retention and Disposition By-law approved by Council and the Records Management Policy in 2003. Automated retention rules for e-mail were implemented as a part of an upgrade to the Exchange Server product in September 2005, to ensure compliance with this by-law and policy.

Management Representation of the Status of Implementation of Recommendation 11 at December 31, 2008

Implementation of this recommendation is considered 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 11

Implementation of recommendation 11 is 100% complete. According to the documents provided, the ITS Department has reviewed the retention periods of e-mails and implemented the current City's retention period requirements in conformity with the City by-laws. The ITS Department should keep up to date with any changes to the City by-laws regulating the City's corporate records. The current retention period is 60 days for corporate e-mails and 90 days for the deleted e-mails. This brings the retention period to five months.

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

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

Management Comment

Management notes that the retention periods noted by the OAG in the assessment for Recommendation 11 are incorrect. They are 60 days for corporate e-mail and 30 days for the deleted e-mails, bringing the retention period to three months.

2005 Recommendation 12

That Information Technology Services review the users with administrator rights on their workstations, and where not justified and required, remove the administrator privileges for that user.

2005 Management Response

Management agrees with this recommendation.

A rigorous documented formal process is followed whenever any user requires local administrative rights.

As part of the Enterprise Security Review project, a review will be conducted regarding administrative access rights for IT Services with recommendations provided to the IT Services Management team in Q1 2006. This review will be repeated on an annual basis.

More restrictive administrative rights for laptop users are being implemented as part of the life cycle laptop replacement program. At this point, funding is available to replace roughly 100 units of the total fleet of 900.

Roughly 50% of the current fleet of City laptops are now running a version of the operating system that offers administrative rights control. IT Services plans to implement these administrative rights restrictions by the end of Q1 2006. The remaining 50% of the City laptop fleet needs to be replaced.

Funding of $700,000 and one (1) additional FTE (or equivalent) will be required in order to accelerate this replacement program to be completed over twelve (12) months. A budget pressure will be identified for the 2007 budget to accelerate this replacement program to be completed over twelve (12) months.

Management Representation of the Status of Implementation of Recommendation 12 as of December 31, 2008

Implementation of this recommendation is considered 100% complete.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 12

Implementation of recommendation 12 is 80% complete. The ITS Department is implementing administrator rights restriction on the hardware that supports the Active Directory GPO control. As for the management's comments, there is no formal process of reviewing of the administrator rights at the local level. The administrator accounts for City and "A domain" administrators are subject of an annual notification. The local administrator accounts are being managed through the Service Desk and there is no annual review. According to the lifecycle hardware replacement program, when the hardware in use will be replaced with systems that support the centralized control over the administrator rights, the ITS Department will be able to review and effectively control the accesses to City owned workstations.

OAG: % complete 80%

Management Representation of Status of Implementation of Recommendation 12 *as of Summer 2010*

Management agrees with the OAG's follow-up audit finding.

ITS is investing in a GRC (Governance, Risk Management & Compliance) tool as part of the PCI DSS (Payment Card Industry – Data Security Standard) compliance program and will leverage this tool to monitor elevated privilege accounts. This will be implemented by the end of Q1 2011.

ITS will continue the existing internal review of its users with local administrator privileges at the workstation level and will work with users to rationalize the business requirement for the continued use or removal of these access roles. Further to this, ITS will look at reviewing our internal policies and procedures with regard to the granting of local workstation administrator privileges.

Management: % complete 80%

2005 Recommendation 13

That Information Technology Services:

a) Review organization roles and responsibilities with accompanying agreements, such as Service Level Agreements (SLAs); and

b) Clearly define roles/responsibilities and define processes to ensure control implementation and monitoring is covered.

2005 Management Response

Management disagrees with these recommendations.

IT Services has reviewed existing organizational roles and responsibilities, and believes that these roles and responsibilities are clearly delineated and effective. Separation of duties and other organizational control mechanisms are fully implemented and maintained across the entire branch.

Management Representation of the Status of Implementation of Recommendation 13 as of December 31, 2008

Implementation of these recommendations is considered 100% complete. This item was discussed at CAWG on March 6, 2007 and was approved by Council on May 9, 2007. It was agreed that:

a) Over the course of 2007/2008, ITS would perform a review of the 2003 IM/IT Security Strategy in order to confirm governance, roles and responsibilities. As well, ITS would adopt the Information Technology Infrastructure Library (ITIL) framework for Information Technology Services, which includes establishing documented operational level agreements (OLA's) between service providers within an organization. The ITIL framework was to be phased-in over the course of 2008/2009.

b) Over the course of 2007/2008, ITS would perform a review of the 2003 IM/IT Security Strategy in order to confirm governance, roles and responsibilities. An internal review of governance, organizational roles and responsibilities was conducted by ITS as agreed at the March 6, 2007 CAWG meeting.

IT believes that these roles and responsibilities are clearly delineated and effective, and appropriate service level agreements are in place. Separation of duties and other organizational control mechanisms are fully implemented and maintained across the entire branch. Nevertheless, new Incident and Change Management processes, consistent with the Information Technology Infrastructure Library (ITIL) framework, have been implemented in key areas of IT and will be fully deployed across the branch by end of Q2 2009 to further streamline and strengthen control mechanisms and governance. In conjunction with the branch's ongoing continuous improvement program, operational agreements and client service level agreements will be reviewed during 2009-2011 for consistency with the ITIL framework, and adjusted as required.

Management: % complete 100%

OAG's Follow-up Audit Findings regarding Recommendation 13

Implementation of recommendation 13 is 100% complete. The ITS Department informed the auditor that there are no internal SLAs defined at the City. On the other side, the roles and responsibilities of the managers, analysts, administrators and other components of the ITS Department are defined and reviewed when needed. The IM/IT Security Standard v1.10 that has been provided to the auditors contains the basic definition of the responsibilities of management roles in the ITS Department, as well as the composition and functions of the IT Services Security Committee (last terms of reference provided for March, 2010).

The auditor obtained and reviewed the job descriptions for operational analysts responsible for monitoring of the City network systems.

OAG: % complete 100%

2005 Recommendation 14

That Information Technology Services develop an Encryption Policy to address key aspects of encryption related to the City's operations and requirements.

2005 Management Response

Management agrees with this recommendation.

Encryption technologies are currently used to safeguard specific systems, but these de facto standards are not presently in one reference document. Existing encryption standards will be collected and documented by Q2 2006.

Management Representation of the Status of Implementation of Recommendation 14 as of December 31, 2008

Implementation of this recommendation is considered 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 14

Implementation of recommendation 14 is 75% complete. The IM/IT Security Standard v1.10 contains the provision of encrypting of sensitive information identified by threat and risk assessments (section 3.5.8 Data Encryption). As of the management comments, no data flow is encrypted. However, compensating controls are present and the perimeter security is ensured.

OAG: % complete ***75%***

Management Representation of Status of Implementation of Recommendation 14 *as of Summer 2010*

Management disagrees with the OAG's follow-up audit finding that implementation of this recommendation is only substantially complete.

The recommendation was to develop an Encryption Policy to address key aspects of encryption related to the City's operations and requirements. This has been fully addressed through the implementation of the Secure File Transfer Protocol (SFTP) which ensures secure transmissions and exchanges of sensitive / confidential files on the City network and /or with the City's partners.

Management considers implementation of this recommendation to be complete.

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

2005 Recommendation 15

That Information Technology Services identify tools for encryption of sensitive e-mail content.

2005 Management Response

Management disagrees with this recommendation.

The revised Responsible Computing Policy, section 7.1, as approved by City Management in September 2005 stipulates that sensitive information is not to be transmitted via the corporate e-mail system.

An enterprise wide e-mail encryption solution would be for internal use only and would not necessarily be compatible with external partners, as there is no national or international standard for e-mail encryption.

Should an enterprise-wide e-mail encryption solution be required, it is estimated to cost $100,000 and require 2 FTEs (or equivalent) to administer. A budget pressure would be identified for the 2007 budget.

Management Representation of the Status of Implementation of Recommendation 15 as of December 31, 2008

Implementation of this recommendation is 20% complete. This item was discussed at CAWG on March 6, 2007 and was approved by Council on May 9, 2007. IT was to evaluate a secure file exchange service that can be used with City business partners to exchange sensitive documents. A project has been launched to implement a hosted external email encryption service. A Request for Proposal is scheduled for release by February 2009, bid evaluations will be completed in March/April 2009, and a contract is expected in May/June 2009.

Management: % complete 20%

OAG's Follow-up Audit Findings regarding Recommendation 15

Implementation status of recommendation 15 is 75% complete. Management disagreed with the initial recommendation and no further action has been taken to implement an e-mail encryption system on the City's network. Management has informed the auditors that an SFTP service that ensures the secure transmission and exchange of files on the City's network and/or with the City's partners has been implemented. However, the e-mail encryption issue is still relevant and no action has been taken to encrypt these exchanges.

OAG: % complete 75%

Management Representation of Status of Implementation of Recommendation 15 *as of Summer 2010*

Management disagrees with the OAG's follow-up audit finding.

In accordance with the CAWG resolution of March 6, 2007, ITS has implemented a Secure File Transfer Protocol (SFTP) service and made all City Management aware of this through a Management Bulletin on May 12, 2010.

An Email encryption service was not within scope of the resolution reached in 2007. It was mentioned in error in the December 2008 status. The solution identified focussed solely on implementing a Secure File Transfer Protocol (SFTP) service.

Management considers implementation of this recommendation to be complete.

Management: % complete 100%

2005 Recommendation 16

That Information Technology Services implement strong encryption on the link between DC2 and the library lab network that uses the Internet for communication.

2005 Management Response

Management agrees with this recommendation.

IT Security will investigate the use of this link and the safeguards currently in place in Q4 2005.

Management Representation of the Status of Implementation of Recommendation 16 as of December 31, 2008

Implementation of this recommendation is considered 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 16

Implementation of recommendation 16 is 100% complete. Management communicated and provided evidence that the link between DC2 and DC4 has been encrypted with 3DES/MD5 at first and then enforced to AES-256/SHA.

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

2005 Recommendation 17

That Information Technology Services:

a) Create a program with annual user IT Security policy review with mandatory quarterly/semi-annually IT Security awareness briefings;

b) Continue the Security flash e-mail awareness campaign notifying users of significant e-mail attacks; and

c) Improve the effectiveness of the IT Security awareness campaign.

2005 Management Response

Management agrees with these recommendations.

A formal IT Security Awareness program already exists. Awareness articles are issued through City Briefs on a monthly basis, Management Bulletins are also issued as necessary, and IT Security awareness briefings occur to address strategic issues or groups. Awareness activities have been part of the annual planning cycle since 2003. Flash e-mail awareness campaigns will continue.

A third party review to measure and assess the current awareness targets and associated delivery strategy was scheduled to begin October 2005 as part of the Corporate IT Security Awareness Program. This review was deferred to 2006 due to a City-wide budget freeze, and will include specific recommendations and a workplan identifying the priority messaging targets.

Management Representation of the Status of Implementation of Recommendation 17 as of December 31, 2008

Implementation of these recommendations is 100% complete.

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

OAG's Follow-up Audit Findings regarding Recommendation 17

Implementation of recommendation 17 is 100% complete. The ITS Department provided the auditors with comprehensive documentation regarding the Responsible Computing Policy awareness campaigns. The awareness campaigns included briefings and management bulletins. An external third party has been retained to evaluate possible improvements of the awareness campaigns and suggest ways to increase the visibility of the security controls to City staff.

The Responsible Computing Policy was last updated in March 2010.

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

2005 Recommendation 18

That Information Technology Services:

a) **Monitor and control the use of the Internet and e-mail usage by City employees;**

b) **Develop appropriate recording tools that provide reliable reporting of e-mail usage;**

c) **Develop and implement a process to provide managers with reports of their staff's Internet and e-mail usage so that management can evaluate if appropriate usage of e-mail and Internet is occurring; and**

d) **Revise the Responsible Computing Policy to limit use of the Internet to mainly business purposes and limit personal usage to incidental or occasional only.**

2005 Management Response

Management agrees with these recommendations.

IT Services uses Websense to monitor and control the use of the Internet at a macro or system level. Prior to the audit, IT Services launched an extensive project to enhance the rigour of the Websense implementation, scheduled for completion in Q1 2006. An extensive range of additional Websense filtering features is now in place that enhances the monitoring of Internet usage and blocking of websites that are not consistent with the Code of Conduct and Responsible Computing Policy. Monthly reviews of Websense reports by IT Services will continue, and changes to categories, website blocking, and follow-up investigations will continue.

In 2006 IT Services will enhance Internet monitoring using existing Websense reporting tools. A detailed analysis of a minimum of 50 Internet accounts will be conducted on a semi-annual basis for compliance with the Responsible Computing Policy. Instances of non-compliance will be investigated in conjunction with managers and the Labour Relations unit within Employee Services Branch. It is projected that this level of review and follow-up will generate the equivalent of 1.5 FTEs (2,700 hours) of staff effort to implement.

IT Services/Labour Relations will be contacting the respective managers of the 50 random and 50 top users generated throughout the audit. IT Services in consultation with Labour Relations will provide the Internet log report along with guidelines on how to interpret the data set and how to approach employees with any concerns that might be presented on their Internet usage.

IT Services will continue to produce management reports and metrics using Promodag, and will investigate additional monitoring tools and reporting capabilities that would enable monitoring of individual e-mail accounts. Evidence of non-compliance with the Responsible Computing Policy will be investigated in conjunction with managers and Labour Relations. At this time, the additional effort to review and follow-up is not known pending identification and selection of new tools. A budget pressure would be identified for 2007 to acquire and implement additional monitoring and reporting tools.

The revised Responsible Computing Policy clearly states that the Internet and e-mail are provided for "legitimate business use in the course of assigned duties and only incidentally for personal use", and that disciplinary action, including dismissal, are consequences of non-compliance. The Responsible Computing Policy will be reviewed to ensure that it applies equally to both Internet usage and e-mail usage, and reflects our current practices.

Management Representation of the Status of Implementation of Recommendation 18 as of December 31, 2008

Implementation of these recommendations is 100% complete. Two Internet usage audits are performed annually: a review of the Top 50 Internet users and a review of a random selection of 50 Internet users. At present, there is no intent to assess e-mail usage. IT engaged Allstream to conduct an email assessment. Their review determined that there is no automated tool to perform this assessment in a cost-effective manner. Any future assessment of e-mail usage will have to be determined on a case-by-case basis, and will take into consideration all applicable policies and legislation, including the City's protection of privacy obligations contained in the *Municipal Freedom of Information and Protection of Privacy Act* and other privacy legislation. Such obligations would necessitate a review of the City's collection and use of any personal information related to the e-mails in question as well as the City's notification obligations in the circumstances.

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

OAG's Follow-up Audit Findings regarding Recommendation 18

Implementation of recommendation 18 is 50% complete. The evidence provided to the auditors reflects that two Internet usage audits are performed annually: a review of the Top 50 Internet users and a review of a random selection of 50 Internet users. The IPCA program that the ITS Department has in place helps identify some of the violations of the Responsible Computing Policy. Through the

IPCA program, the managers are informed of their staff Internet usage. Through the Websense reporting tool, the ITS Department can access any user's Internet activity. The only limitation is the log retention period. It is strongly recommended that the IPCA program be continued and its scope might be extended to the first 100 users. Given that the City has in excess of 9,000 network users, 50 user logs represent only 0.55% of the users.

The ITS Department might consider extending the sampling to 2.5% of the users, which would bring the total number of reviewed logs to approximately 225. This would result in a broader coverage as well as a larger selection of random users.

The monitoring does not provide a comprehensive view of the Internet and e-mail usage of the whole user community. The e-mail monitoring is not in place. The ITS Department contracted a third party to evaluate the possibility to implement e-mail monitoring tools and the conclusions of the study show that presently there is no available automatic tool to perform an adequate analysis of the business and personal e-mail use. The ITS Department uses Promodag, which is an e-mail reporting tool that is used mainly in reaction to incidents e.g., exceeding the mailbox limit. As to the third party report, the Promodag tool can be used for various report production. Although it lacks the capability to automatically distinguish personal vs. business e-mail usage, per user and per department e-mail usage reports can be produced. Thus, Promodag could assist identify the e-mail usage of a user that is targeted as not respecting the Responsible Computing Policy.

It should be noted that the Internet and e-mail monitoring tools are used for incident monitoring and not for operational usage monitoring. The operational monitoring of user activity would provide a better understanding of the Internet and e-mail usage on the City network but will necessitate a change of philosophy relating to monitoring. The City could decide on this change of principle and act accordingly for the implementation.

As part of the follow-up audit, the OAG contracted with an outside specialized firm to do a detailed review of Internet usage at the City. The full report was provided to management for their information. The firm reviewed a sample of 1,000 users' Internet usage in June 2010. They found that Internet usage was generally in accordance with City policies.

During the review of Web site usage, it was found that some users had access to Web email sites such as Hotmail, Yahoo and gmail. Access to these sites is generally not permitted under City policy. The City should review which users had these accesses and if these exceptions are permitted under City policy.

Another issue identified is that at the time of the audit, the City was using Websense Version 6.3.1. Since then, Websense has released several other versions: 6.3.3, 7.0, 7.1, 7.5 and 7.6. The most current version is 7.6. Consideration to upgrading the version of Websence used may be warranted.

OAG: % complete ***50%***

Management Representation of Status of Implementation of Recommendation 18 *as of Summer 2011*

Management agrees with the OAG's follow-up audit finding, however, the portion of the recommendation not yet complete is not practical or cost-effective to implement.

As noted in the December 2008 status, IT engaged Allstream to conduct an email assessment. Their review determined that there is no automated tool to perform this assessment in a cost-effective manner.

Further, management has clarified its position on Websense in an earlier communication with the OAG:

"The City's Internet filtering service, Websense, is a tool designed first and foremost for security purposes to safeguard the City's network from dangerous (malicious and compromised) Internet sites. It is also used to restrict access to web sites with inappropriate content, consistent with City policy and Management direction.

The Internet access logs generated by this tool can be easily misinterpreted and used in a manner that does not reflect their true content, given the purpose and design of the Internet filtering tool and the nature of today's Internet web site technology & Internet browsers. "

With regard to the recommendations found in the OAG's assessment, ITS notes that access to third party webmail services such as Hotmail, have been granted to specific individuals within the corporation as exceptions to the Responsible Computing Policy based on the business need of those individual users. These exceptions have been reviewed and approved by the IM/IT Security Section and are documented. Also of note, the ITS department is in the process of upgrading the Websense security system to the latest version and plans to have this work completed before the end of 2011.

Management considers implementation of this recommendation to be complete.

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

4 SUMMARY OF THE LEVEL OF COMPLETION

1. The table below outlines our assessment of the level of completion of each recommendation as of Spring 2010.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	7b, 7f	2	5%
Partially Complete	50 – 74	18a, 18b, 18c, 18d	4	10%
Substantially Complete	75 – 99	7c, 7g, 12, 14, 15, 21a*, 21b*, 21c*	8	19%
Complete	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 16, 17a, 17b, 17c,19a*, 19b*, 20*	27	66%
TOTAL			41	100%

2. The table below outlines management's assessment of the level of completion of each recommendation as of Summer 2010 in response to the OAG's assessment. These assessments have not been audited.

Category	% Complete	Recommendations	Number of Recommendations	Percentage of Total Recommendations
Little or no action	0 – 24	-	-	-
Action Initiated	25 – 49	7b, 7f	2	5%
Partially Complete	50 – 74	-	-	-
Substantially Complete	75 – 99	7c, 7g, 12, 21a*, 21b*, 21c*	6	15%
Complete	100	1, 2, 3, 4a, 4b, 5a, 5b 6a, 6b, 7a, 7d, 7e, 7h, 8a, 8b, 9, 10, 11, 13a, 13b, 14, 15, 16, 17a, 17b, 17c, 18a, 18b, 18c, 18d, 19a*, 19b*, 20*	33	80%
TOTAL			41	100%

*Confidential recommendations are omitted from this report as they contain information that could compromise the City's information technology security.

CONCLUSION

Most of the recommendations from the 2005 Audit of Internet Usage and Controls have been implemented by the Information Technology Services (ITS) Department. The main issues identified relate to monitoring of staff Internet and e-mail activity. In 2009, two Cisco PIX firewalls were nearing the end of their useful life and manufacturer's support and have been replaced by newer ASA firewalls in 2010. This will offer increased stability and manufacturer support in case of incidents. There was no Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) on the network at the time we conducted this followi-up audit, but the ITS

Department is in the process of implementing such devices. These efforts align with the implementation of the Payment Card Industry (PCI) requirements which the City of Ottawa is subject to.

The requested Websense reports containing City staff's Internet use could not be provided due to technical difficulties. The ITS Department is deploying its efforts to provide these documents and these will be reviewed. As is, the City of Ottawa internal network generally meets industry best practices for secure architecture and use of appropriate protection technologies. The Security Information and Event Management (SIEM) project will add strength from a security standpoint to the City's network, considering the IDS/IPS devices are part of the implementation.

There is no evidence that sensitive information is being encrypted on the City network. No document has been provided indicating information classification and/or guidelines for its handling. Implementation of PCI requirements will require such tools; as a minimum for banking and personal data that is transmitted over the City network. Once implementation of current PCI requirements is achieved, these deficiencies will probably be rectified.

5 ACKNOWLEDGEMENT

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

.