CITY OF HAMILTON
CITY MANAGER'S OFFICE
Audit Services

TO:	Chair and Members Audit, Finance and Administration Committee
COMMITTEE DATE:	May 12, 2014
SUBJECT/REPORT NO:	Audit Report 2013-10 – Corporate Services – Information Security and Identity & Access Management Review (AUD14014) (City Wide)
WARD(S) AFFECTED:	City Wide
PREPARED BY:	Ann Pekaruk 905-546-2424 x4469
SUBMITTED BY: **SIGNATURE:**	Ann Pekaruk Director, Audit Services City Manager's Office

Discussion of Private and Confidential Appendix "A" to Report AUD14014 in Closed Session is subject to the following requirement(s) of the City of Hamilton's Procedural By-law and the Ontario Municipal Act, 2001:

- **The security of the property of the municipality or local board.**

RECOMMENDATION

(a) That the Management Action Plans, as detailed in Private and Confidential Appendix "A" of Report AUD14014 be approved;

(b) That the General Manager of Finance and Corporate Services be directed to instruct the appropriate staff to have the Management Action Plans (attached as Private and Confidential Appendix "A" to Report AUD14014) implemented; and

(c) That the Appendix "A" to Report AUD14014, respecting Audit Report 2013-10 – Corporate Services – Information Security and Identity & Access Management Review, remain confidential and restricted from public disclosure.

EXECUTIVE SUMMARY

The 2013 Internal Audit work plan approved by Council included a review of Information Security and Identity & Access Management. Information Security deals with the protection of information and information systems against unauthorized access or modification. The scope for the Information Security portion of the review included an

evaluation of management and business processes relating to the external facing network.

Identity and Access Management is the security discipline that enables the correct individuals to access the appropriate resources at the right times for justifiable reasons. The scope for the Identity & Access Management portion of the review included detailed testing for all areas that were the responsibility of the Information Technology (IT) Division and additional limited testing if governance issues were identified.

Both topics included a review of key risk areas to determine if these are being appropriately mitigated and identify any weaknesses or deficient business process controls. Recommendations were made to safeguard assets and information and identify any weaknesses in workflows to strengthen controls.

The results of the review are presented in a formal Audit Report (2013-10) containing observations, recommendations and management responses. Audit Report 2013-10 is attached as Private and Confidential Appendix "A" to Report AUD14014.

Alternatives for Consideration – Not Applicable

FINANCIAL – STAFFING – LEGAL IMPLICATIONS (for recommendation(s) only)

Financial: The implementation of several of the recommendations will require funding. For example, the IT Governance work, the Threat Risk Assessment and the Employee Security Awareness Program will require both capital and operating budgets. As such programs are in their very early stages, at best, it is difficult to ascertain the dollars that will be required. However, as each project is planned, funding requests will come forward to Committee and Council.

Staffing: Many of the projects proposed are of a long term nature and will require involvement of internal staff. Reassignment and secondment of current staff and possibly hiring of additional new staff may be necessary. Again, once the planning has been completed, any staff requirements will be brought forward to Council.

Legal: None.

HISTORICAL BACKGROUND (Chronology of events)

This review was scheduled as part of the 2013 Internal Audit work plan approved by Council. Fieldwork was completed in October to December 2013. An information session on the topics reviewed was presented to SMT in March 2014. The results of this review are attached as Private and Confidential Appendix "A" of Report AUD14014.

The Audit, Finance and Administration Committee receives and approves final audit and review reports as part of its responsibilities for the oversight of governance and control.

POLICY IMPLICATIONS AND LEGISLATED REQUIREMENTS

City of Hamilton Information Technology Security Policy

City of Hamilton Password Policy

City of Hamilton User Account Policy

City of Hamilton Security Incident Response Policy

Payment Card Industry Data Security Standard (PCI DSS)

RELEVANT CONSULTATION

Private and Confidential Appendix "A" to Report AUD14014 includes action plans which reflect the responses of the IT Division, Finance and the Senior Management Team (SMT). Due to the complex nature of the activities reviewed and the subsequent recommendations that were made, SMT was asked to provide action plans for items with a corporate-wide impact and IT Governance implications.

ANALYSIS AND RATIONALE FOR RECOMMENDATION (Include Performance Measurement/Benchmarking Data if applicable)

The City of Hamilton has a complex information technology infrastructure environment. Corporate-wide information security services are provided by the IT Division's Security Section. Areas monitored and reported upon regularly by the Security Section include: malware detections, antivirus compliance, patching compliance and internet email volumes. There is also a detailed and complex security monitoring program that is executed daily by the Security Section and includes: monitoring physical security, firewalls, data security and corporate user accounts. The monitoring program consists of a formalized and scheduled routine of "security checks".

Between 2011 and 2013, there has been an average of approximately two security incidents per year that required a response from the Security Incident Response Team (SIRT) at the City of Hamilton. The severity and operational impact of a single security incident that requires a response from the SIRT can vary from being fairly minimal to an incident that could potentially cripple the City's operations.

The scope for the Information Security portion of the review included management and business processes relating to the external facing network. The scope for the Identity and Access Management portion of the review included detailed testing for all areas that were the responsibility of the Information Technology (IT) Division and additional limited testing if governance issues were identified during this initial evaluation.

The review focused on risk assessment, the monitoring of security and access controls and the evaluation of business process controls and procedures.

The review identified opportunities to improve controls, strengthen management oversight, safeguard the City's information and technology assets and improve IT governance.

A formal Audit Report (2013-10) containing observations, recommendations and resulting management action plans was issued. Seventeen recommendations were included in Audit Report 2013-10 (attached as Private and Confidential Appendix "A" to Report AUD14014).

Audit Services conducted this review in conformity with the *International Standards for the Professional Practice of Internal Auditing*. These standards require that Audit Services plan and perform the review to obtain sufficient, appropriate evidence to support the findings and conclusions based on the review objectives. Audit Services believes that the work performed provides a reasonable basis for the review findings and conclusions.

ALTERNATIVES FOR CONSIDERATION

(Include Financial, Staffing, Legal and Policy Implications and Pros and Cons for each alternative)

Not applicable

ALIGNMENT TO THE 2012 – 2015 STRATEGIC PLAN

Strategic Priority #2

Valued & Sustainable Services

WE deliver high quality services that meet citizen needs and expectations, in a cost effective and responsible manner.

Strategic Objective

2.1 Implement processes to improve services, leverage technology and validate cost effectiveness and efficiencies across the Corporation.

Strategic Priority #3

Leadership & Governance

WE work together to ensure we are a government that is respectful towards each other and that the community has confidence and trust in.

Strategic Objective

3.4 Enhance opportunities for administrative and operational efficiencies.

APPENDICES AND SCHEDULES ATTACHED

Private and Confidential Appendix “A” to Report AUD14014.

ap:bm