CITY OF Burlington

**SUBJECT: External audit results for 2016**

**TO: Audit Committee**

**FROM: Finance Department**

Report Number: F-27-17

Wards Affected: not applicable

File Numbers: 430-04

Date to Committee: May 31, 2017

Date to Council: June 12, 2017

## Recommendation:

Receive and file finance department report F-27-17 presenting information on the external audit results for 2016.

## Purpose:

An Engaging City

- Good Governance

## Background and Discussion:

The Audit Committee is responsible for the oversight of all audit matters including the annual audit of the City and local boards' financial statements.

To assist with this responsibility, the external audit management letter for the City is presented for Committee's information.

Recommendations provided by the external auditors on internal control enhancements, as they relate to the audit, is one of the benefits of annual financial statement audits.

The auditors' Management Letter provides committee with the auditors' findings in their review of internal controls that affect the audit. The management responses outline action plans to address these internal control enhancement opportunities as identified by the auditors.

The audit points relate to the audit of ITS operations and responses are those of ITS management. There were no audit points directed to Finance management for the 2016 external audit. The audit points and responses are as follows:

## 2016 Audit Points

## SAP Excessive Privileged Access

### Observation

Excessive SAP (the City's financial system) access is granted to 12 users, including 10 IT users and 2 business users. Access privileges distributed to these users include debugging access, all-transaction access, and role and user maintenance access.

### Implication

Excessive access may be used to execute any transaction/program, modify programs, directly maintain table data, and/or assign unauthorized access privileges. This may lead to bypassing of segregation of duty (SOD) controls and/or performing unauthorized changes to financial data.

### Recommendation

Excessive access should not be assigned to any users and administrative access should be highly restricted based on users' SAP administration responsibilities. If excessive access is required, it should be granted through an emergency process or a temporary role assignment process.

### Management Response

All access to the SAP application was reviewed resulting in one IT account being disabled and one business account being modified to remove specific privileges. The other accounts were reviewed and it was determined that the access was justified based on their job responsibilities or roles as part of the application support team and current support practices for the SAP application.

The current practice, as documented in SOP-047 SAP Systems Authorizations Principal of Least Privilege, was put in place to ensure that Region of Halton staff along with City of Burlington Finance and ITS staff have a documented process for managing account access in the production environment.

As a best practice, a review of the current process for SAP access should occur with key staff from the Region of Halton and City of Burlington to identify areas of improvement to bring our current process closer to standard best practices.

Responsible party: Manager Business Application, Controller and Manager of Financial Services

***Timing: June 2017***

## SAP Change Management Access

### Observation

Access and related settings do not enforce a change management process for SAP. Nine (9) users, including 8 IT users and 1 business user, have unauthorized change management access. This includes access to modify change control settings, develop directly in production, transport changes into production, as well as access developer keys. It was also noted that there is limited logging relating to the SAP change management process.

### Implication

Inappropriate assignment of change management access increases the risk of inappropriate changes to application systems or programs that contain relevant automated controls and/or report logic. Additionally, in the absence of a change monitoring process, any unauthorized changes may not be detected.

### Recommendation

Change management access (including access to developer keys and to modify change control settings) should be highly restricted (based on job responsibilities), and the use of such access should be fully logged and monitored.

Segregation of duty controls should also be enforced. No users should have access to directly develop in production. Furthermore, developer keys should not be assigned in production, and users with developer keys should not have access to transport changes into production.

### Management Response

Access to the SAP environment has been set to non-modifiable resulting in changes to the production environment only being allowed through transports (pre-programmed code). Identification of an existing account with developer key access has been acted upon with this access being immediately revoked. Access to run transports are currently restricted to a limited number of staff at the Region of Halton, none of whom have developer key access.

Additionally, this observation and resulting recommendation had been previously made during an internal audit of the SAP system completed by Deloitte at the request of the City Auditor in late 2013. At that time, discussions were held with the Basis group at the Region of Halton. They indicated that a number of system administration transactions are run to monitor and control the system on a daily basis. This process is still in effect today.

The current process, as documented in SOP-047, needs to be reviewed to ensure that control settings along with the appropriate segregation of duties is being monitored appropriately as part of the procedure.

Responsible party: Manager Business Applications, Controller and Manager of Financial Services.

***Timing: June 2017***

## Avantis User Reviews

### Observation

Application user reviews were not performed for Avantis, the City's workorder management system, in 2016.

### Implication

With no consistent, coordinated and documented process to regularly, periodically and consistently review user access, there may be an increased risk that unauthorized user accounts may have access to Avantis.

### Recommendation

Management should establish a periodic review process to ensure that only authorized users have access to Avantis.

### Management response

IT staff have acknowledged that the necessary user access review for Avantis was not completed in 2016. A detailed review of the user access privileges was not possible due to the highly complex field level access settings. This results in a very onerous and time consuming manual review of the various access privilege screens with both IT staff and the appropriate business staff working together. As a result, IT staff will focus the access review at the application level to ensure that only approved users can access the application allowing for a streamlined scheduled process to be put in place.

Responsible party: Manager Business Applications

***Timing: October 2017***

## Conclusion:

Staff appreciates the recommendations provided by the external auditors. Practices have been put in place or will be put in place in the near future to mitigate risk, reduce likelihood of occurrence, and to improve operational effectiveness.

Respectfully submitted,

Sandy O’Reilly

Controller and Manager of Financial Services

905-335-7600 x 7648

## Report Approval:

All reports are reviewed and/or approved by Department Director, Director of Finance and Director of Legal.  Final approval is by the City Manager.