For Action

PricewaterhouseCoopers LLP 2018 Management Letter Follow-up Report

Date: September 19, 2019
To: TTC Audit & Risk Management Committee
From: Chief Financial Officer

Summary

This report outlines a status update on the management letter on internal control recommendations issued by TTC's external auditors, PricewaterhouseCoopers LLP (PWC), in their 2018 year-end audit results report.

Recommendations

It is recommended that the Audit & Risk Management Committee:

1. Receive the report; and

2. Approve forwarding a copy of the report to the TTC Board and then to the City Clerk for submission to the City of Toronto's Audit Committee for information.

Implementation Points

This report must be received at the September 19, 2019 TTC Audit & Risk Management Committee meeting and the September 24, 2019 TTC Board meeting to ensure timely submission to the City of Toronto Audit Committee so that TTC's management letter update is received within six months after its issuance.

Financial Summary

The recommendations in this report have no funding implications.

Equity/Accessibility Matters

This report and its recommendations have no accessibility or equity issues or impacts.

Decision History

In accordance with City Council approval of the Audit Committee July 2004 Report 4, Clause 2 Recommendation 3, the TTC is required to provide an update of outstanding issues raised in the management letter, within six months after its issuance.

https://www.toronto.ca/legdocs/2004/minutes/committees/au/au040713.pdf

Furthermore, at its meeting on February 9, 2017, the TTC Audit & Risk Management Committee approved its terms of reference to include a requirement to "understand the scope of internal and external auditors' review of internal control over financial reporting, and obtain reports on significant findings and recommendations, together with management's responses".

http://www.ttc.ca/About_the_TTC/Commission_reports_and_information/Committee_meetings/Audit_Risk_Management/2017/February_9/Reports/2_TTC_Audit_%20and_Risk_Management_Committee_Terms_Of_Referenc.pdf

Issue Background

The 2018 year-end PWC audit results report, presented at the June 3, 2019 TTC Audit Committee meeting, included a management letter with internal control recommendations and management's initial response to these recommendations.

http://www.ttc.ca/About_the_TTC/Commission_reports_and_information/Committee_meetings/Audit_Risk_Management/2019/Jun_3/Reports/2_PWC_Audit_Results_Report_on_the_TTC_YE_2018.pdf

Comments

The attachment to this report includes PWC's internal control recommendations, management's initial response and a status update detailing the actions taken thus far to address each of the recommendations.

All actions taken to date will be subject to review by PWC during the 2019 external financial statement audit.

Contact

Alex Cassar, CPA, CA
Director, Budgets, Costing & Financial Reporting
416-393-3647
Alex.Cassar@ttc.ca

Signature

Josie La Vita
Chief Financial Officer (Acting)

Attachments

PricewaterhouseCoopers LLP 2018 Management Letter with August 2019 Update

PricewaterhouseCoopers LLP 2018 Management Letter with August 2019 Update

1. *User Access assigned in certain SAP profiles is not appropriately restricted*

Observation

For 16 user accounts in SAP, it was noted that they were not configured with appropriate access restrictions. This allows some of the users to have super user access via a system-wide access profile, as well as others having the ability to edit production data, or to make direct changes to roles in the production environment.

Implication

Accounts with pervasive and powerful access may be misused to edit data, access confidential or financially significant information, and make inappropriate changes to roles by circumventing authorization checks and change management controls.

Recommendation

Management should consider removing all unnecessary access for these accounts. Should there be a need for certain users to maintain this access, a review controls should be implemented to monitor all changes made directly in the production environment to ensure there are no inappropriate changes made.

Management response at June 2019

Management has removed 4 users' access. The remaining 12 users are production support team members who are SAP System Administrators or SAP Security Administrators and require this level of access to properly monitor and support the production systems for daily operations/ incidents. Therefore, the 12 operational production support users cannot be removed. Management will also put in place the recommended monitoring controls to review the changes made directly in the production environment. Monitoring controls will be implemented as soon as possible and no later than Q3 2019.

August 2019 Update

Where applicable, all access has been removed to prevent direct changes in the production system. Users that still have this access, as noted above, require this for production support. It should also be noted, the production system and its configuration is always locked, which prevents any direct changes from being made regardless of access. In the event of any changes that may be made, they will be tested in the non-production environment and approved by the business owners, prior to being moved to production.

Status

Complete

2. Firefighter account process does not include a review process for the use of the accounts

Observation
Management has not implemented a control activity whereby a supervisor is responsible for reviewing the transactions/ activities performed by the firefighter account in order to validate whether it aligns with the use of that access. (Note: a firefighter account has elevated privileges that will be provisioned to approved users upon production emergencies.)

Implication
The lack of review control over the activities performed by elevated firefighter accounts introduces the possible risk of unauthorised transactions being processed after the access is provisioned.

Recommendation
Management should consider implemented a control to review the transactions performed by firefighter IDs on a "per instance" basis (i.e. every time that the firefighter ID is used.) Evidence of review should be documented and retained by management.

Management response at June 2019
Management has commenced implementing a control to review transactions performed by firefighter IDs and documenting evidence of this review. The implementation of the new process will be completed by Q3 2019.

August 2019 Update
TTC has implemented a new process for changes performed by firefighter IDs. On a weekly basis, firefighter logs are generated and are reviewed by Finance and Payroll staff to mitigate the risk of unauthorized transactions being processed.

Status
Complete

3. *User accounts of terminated employees are not removed from SAP and SuccessFactors application on a timely basis*

Observation

It was noted that across the population of users with access to SAP (Payroll and Finance) and SuccessFactors, there were 10 terminated users who continued to have access to SAP and 13 users who continued to have access to SuccessFactors subsequent to their termination from TTC.

Implication

Without timely removal or disabling of terminated employees, dormant accounts of terminated employees may be misused in the applications. Additionally, this may result in terminated employees being paid (both salaries and/or benefits) after their termination dates.

Recommendations

1. Management should continue to monitor users with active access to SAP and SuccessFactors and consider implementing an account expiry for terminated user accounts within a reasonable period after termination date in order to remain consistent with TTC policies.

2. Management should also consider implementing a periodic review control process to review the list of terminated employees against key financial applications.

Management response at June 2019

As of May 1, 2019, IT management has removed/ revoked the access of the terminated users. There are other mitigating controls including physical access controls to a TTC laptop and/or desktop, security passes and security controlled areas that significantly reduce the probability of SAP accounts being accessed by former employees.

When employees move within the organisation, Access Control Administration validates whether existing access to systems is to be maintained, with the new department’s IT representative. If access is no longer required as part of the employee’s new role, it is removed at that time. With respect to terminated employees, Access Control Administration receives notice of terminated employees and takes action to remove their access accordingly.

In addition, management in Payroll will maintain a list of all employees with access to ECC (SAP Payroll), including their job classification information, and implement a review to validate that existing users have not changed roles since the previous review. Users who have changed roles will be contacted and if their access requirements have changed they will be asked to reapply. If they still require the same access, they will be required to re-obtain approval from their department head confirming this to be the case. As part of the review, the Payroll business team will also validate that access for terminated employees has been removed.

August 2019 Update
The Payroll department has implemented a monthly review process of users with active access and the first review will be performed in September. The Finance department is developing an annual review process which will be finalized and approved by end of September. The first review of Finance users with active access will be performed in December 2019.

Status
In Progress

4. *Certain employees have access to maintain employee master data and execute payroll process (segregation of duties)*

Observation
It was noted that there are 8 users with the ability to maintain employee master data (i.e. edit time) and to execute pay run, which present a segregation of duties conflict. Users with conflicting access include 6 employees who do not require access to execute pay run. For the remaining 2 users, they require access to both functions in order to lock employee records (where necessary) before the pay run.

Implication
There is a risk that a single user may perform unauthorized changes to master data information (i.e. pay rates) and execute the pay run process, which would impact financial reporting.

Recommendation
Management should consider changing the roles of these users to resolve the segregation of duties conflicts. If management does not change the roles of these users, they should consider implementing a monitoring or review control to mitigate this risk.

Management response at June 2019
Management is aware of the conflicting access rights, and for employees who do not require access to execute pay run, they have initiated a request to update the users' roles to eliminate this conflict for 6 of the 8 users. For the remaining 2 users who require access to both employee master data as well as executing payroll, management will include a new review control to identify any hours that may have been directly changed in SAP. This review control will be performed by the Payroll Manager each payroll cycle commencing pay ending May 4, 2019.

August 2019 Update
Management has removed access of the 6 users to execute pay run. The reconciliation control has been put in place to identify any hours that may have been directly changed in SAP. Payroll reconciles the total hours captured in the legacy system compared to the hours received by SAP. Any discrepancies are investigated and resolved. The reconciliation is reviewed by the Payroll Manager.

Status
Completed

5. SuccessFactors workflows are not appropriately configured

Observation
It was noted that workflows in SuccessFactors were configured with the Service Centre Coordinator as the last person in the workflow with access to “edit without route change”. This setting allows the Service Centre Coordinator to edit and already submitted or approved request without the need to re-route the request for approval.

Implication
There is a risk that the Service Centre Coordinator may erroneously or maliciously edit an already approved workflow that could result in financial impact during the payroll process.

Recommendation
Management should consider implementing a monitoring or review control to mitigate this risk.

Management response at June 2019
Management confirmed that the workflows are required to be configured in this manner because the Service Centre Coordinator requires such edit access to support the business process. Any change is auditable in SuccessFactors and will be monitored by the Employee Service Centre Manager to ensure it is being used appropriately. Management is aware of and accepts the risk, as they determine that the guidelines around how edit access is used and the auditability of the data changes provide sufficient compensating controls in the process.

Status
Complete