TECHNOLOGY & INNOVATION
WINDOWS SECURITY REVIEW
AUDIT 19-11
July 30, 2019

CITY OF TAMPA

Jane Castor, Mayor **Internal Audit Department**

Christine Glover, Internal Audit Director

July 30, 2019

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Windows Security Review, Audit 19-11

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Technology & Innovation, Windows Security Review.

We thank the aforementioned management and staff for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: Dennis Rogero, Chief of Staff
Sonya Little, Chief Financial Officer
Russell Haupert, Chief Technology Officer
Ernest Mueller, Chief Assistant City Attorney
Martin Zinaich, Information Security Officer

TECHNOLOGY & INNOVATION
WINDOWS SECURITY REVIEW
AUDIT 19-11

/s/ Anthony D. Tiwari

Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION
WINDOWS SECURITY REVIEW
AUDIT 19-11

BACKGROUND

The Technology & Innovation (T&I) Department's Information Security Office (TISO) was established to ensure the security of the City of Tampa's (COT's) information and technology assets. To accomplish this, one top goal of TISO is to fully implement an Information Security Program at COT[1]. The five-person team coordinates the development of security policy guidelines, enforces network access rules, identifies, and mitigates complex threats to ensure the seamless and secure operation of COT's network.

The network runs on a Microsoft Windows operating system and uses Active Directory (AD) as the underlying technology to provide an integrated sign-on system that addresses security, access, and identity management. AD provides a central repository that contains user identifications, user permissions, and audit processing. Furthermore, AD allows for the centralized management of users and their security in alignment with information security frameworks[2]. To accomplish management's initiatives, the International Organization for Standardization (ISO) 27001 framework is primarily used. ISO is an internationally recognized standard designed for organizations as a reference for implementing and managing information security controls[3]. The standard provides TISO comprehensive guidance for establishing and maintaining information security processes.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY19 Audit Agenda. The objectives of the audit were to assess:

1. That TISO policy and procedures manual contained detailed and consistent internal processes.
2. That AD access is explicitly controlled and monitored.
3. The processes for adding, transferring and removing users from the network.
4. The application of timely security patches and updates to employee's computers.
5. The physical security of premises, buildings and areas that contain server equipment.
6. The formal incident reporting process.
7. The results of penetration tests conducted by a third party organization.
8. The process for granting and monitoring all non-COT employees that require network access.
9. The process of employee training and awareness programs.
10. That a periodic user access review is performed for all users including privileged accounts.

---

[1] Retrieved on 4/30/2018 from: https://itampa.ads.cot/technology/security-office.
[2] Windows AD Assurance Review, Control Objectives for Information and Related Technologies.
[3] International Organization for Standardization, ISO 27001 and ISO 27002 Manual.

STATEMENT OF SCOPE

The audit period covered 2017 and 2018. Both qualitative and quantitative assessments were performed to determine whether the management and staff of TISO were fulfilling their stated duties and responsibilities in an effective and efficient manner. Original records as well as copies were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

We achieved our audit objectives by utilizing the following methods:

1. Conducted interviews with TISO to gain an understanding of internal controls.
2. Researched ISO 27001 and 27002 frameworks to gain an understanding of the management of information security processes.
3. Reviewed internal policy and procedures manuals to determine alignment to the framework.
4. Performed a data reliability analysis to determine completeness and accuracy of system generated information used by management.
5. Performed a walkthrough of buildings and areas that contain server equipment to determine that access is secured, justified, and monitored.
6. Reviewed security threats to determine the effectiveness of the incident reporting process.
7. Examined the results of penetration tests conducted by a third party organization.
8. Analyzed a sample of the population of non-COT employees that require access to systems and data.
9. Analyzed the process for training and awareness of information security, from an end user's perspective, to determine conformance with the framework.
10. Analyzed periodic user access reviews to determine the effectiveness and precision of the control.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

AUDIT CONCLUSIONS

Based upon the audit work performed, our conclusions are as follows:

1. TSIO policy and procedure manual contained detailed and consistent internal processes.
2. AD access is explicitly controlled and monitored by the IS team using both manual and automated processes to rapidly identify deviations and take appropriate action.
3. The process for adding, transferring, and removing users from the network is methodical and well defined.
4. The application of timely security patches and updates to employee's computers is completed using centralized configuration in accordance with Windows Security guidelines.
5. The physical security of premises, buildings, and areas that contain server equipment are secured, controlled, and monitored to ensure seamless continuity of operations.
6. The formal incident reporting process has been established and is operationally effective.
7. The results of penetration tests conducted by a third party organization displayed no significant vulnerabilities.
8. The process for granting and monitoring all non-COT employees that require network access is adequate.
9. The process of employee training and awareness programs has not been developed to include all COT employees.
10. The periodic user access review is performed for all users including privileged accounts; however, the review lacked documentation and management's approval.

TRAINING AND AWARENESS

STATEMENT OF CONDITION: For the audit period it was noted that a segment of current employees were not formally trained on awareness of information security threats. T&I and Tampa Police Department employees are trained on their responsibilities and obligations to support the City's Information Security Policy. However, all employees are not trained on awareness of information security threats in the course of their normal work and ways to reduce the risk of human error.

CRITERIA: The ISO 27001 framework used by TISO - Section A.8.2 describes that during employment, all employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

CAUSE: Policies and Procedure documents are made available together with periodic email notifications distributed by TISO. However, these documents may be overlooked as a system of formal training has not been implemented, for all employees and contractors, to mitigate the risk of human error. Further noted in 2016 a project was started by T&I to implement a third party training program which has not materialized. This was partially due to external sharable content compatibility issues in Oracle.

EFFECT OF CONDITION: Employees are considered the weakest link of any organization and may be unaware they are allowing a hacker access to their system. Security breaches and hacking events are costly and may lead to permanent loss of sensitive data. Employees may not be familiar with the information security policies and best practices that govern the use of IT assets and how to prevent or detect a potential breach.

RECOMMENDATION 1: TISO should consider a more proactive approach by developing a new hire and annual ongoing training program. This could be developed internally and conducted through the Oracle Employee Development Portal, for all new/current employees and contractors. Training could then be distributed in an Oracle online lab session for users to certify participation and understanding.

MANAGEMENT RESPONSE: Management agrees, and in 2016 project 100311 was initiated to add a formal training option to the internal education efforts already in use. Regrettably, internal processes beyond the purview of the T&I Security Office caused a delay in project execution. While the recommendation to develop internal training is noted, management feels the current path of providing training from a professional security educational content provider is still the best course. Additionally, the use of targeted training which requires user interaction should provide a better educational conveyance. It is our understanding that the issues preventing implementation of this important portion of our security plan have been eliminated and that the program will proceed as originally indicated.

TARGET IMPLEMENTATION DATE: Initial Rollout and Pilot by June 28, 2019 with City mandate for training and all employee completion by December 31, 2019.

PRIVILEDGED ACCESS REVIEW

STATEMENT OF CONDITION: Quarterly privileged access reviews for networked systems were performed for the audit period 2017 and 2018 that, while compliant with Criminal Justice Information Services (CJIS) and Payment Card Industry (PCI) requirements, lacked a fully documented artifact with management approval. It was noted that TISO uses an application to monitor and send notifications in the event an administrator account is created or added to a group. However, the manual process of performing the privileged access review control would be improved with comparison to a known good source of employee data and an authorized signature.

CRITERIA: The ISO 27001 framework used by TISO - Section 11.2.4 Review of user access rights, describes that management should review users' access rights at regular intervals using a formal process. The authorizations for special privileged access rights should be reviewed at more frequent intervals, e.g., at a period of 3 months; privileged allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained.

CAUSE: A well-defined process has not been created to document and extend the privilege access review control in conformance with TISO's internal framework standards.

EFFECT OF CONDITION: Domain Administrator accounts have access to all workstations and servers which can control system configurations, administrative accounts and domain group membership. Local Administrator accounts have administrative control over specific servers or local workstations and the information stored there. Both privileged accounts have the highest level of control over systems and data; any unauthorized access to, and modifications from, these accounts can have serious consequences.

RECOMMENDATION 2: TISO should consider developing a more robust process to perform the quarterly review of AD administrator accounts. This should comprise of identifying the appropriateness of each privileged user to include management's sign off.

MANAGEMENT RESPONSE: Management agrees with these findings. As noted, the City's audits of this area were and are conducted annually during CJIS or PCI audits along with periodic manual reviews. We also recognize the benefit of account review under the principle of least privilege (PoLP), as in aforementioned manual quarterly review. Corrections are already underway. The proactive account alerts will continue as part of a more proactive approach to security.

TARGET IMPLEMENTATION DATE: Effective immediately, the security office ensure that quarterly reviews are reviewed and compared to a known good source with appropriate management approval. By Oct 1, 2019 will have a fully documented process that generates an artifact of the privileged access review with the designated authorized signature.