

**TECHNOLOGY AND INNOVATION
INFORMATION SECURITY OFFICE
SECURITY POLICIES AND
INFORMATION TECHNOLOGY PROCEDURES
AUDIT 16 – 09
AUGUST 17, 2016**



CITY OF TAMPA

Bob Buckhorn, Mayor

Internal Audit Department

Christine Glover, Internal Audit Director

August 17, 2016

Honorable Bob Buckhorn
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Security Policies and Information Technology Procedures, Audit 16-09

Dear Mayor Buckhorn:

Attached is the Internal Audit Department's report on Security Policies and Information Technology Procedures.

We thank management and staff of Technology and Innovation Department 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 Hauptert, Director of Technology and Innovation Department
Martin Zinaich, Information Security Officer, Technology and Innovation

**TECHNOLOGY AND INNOVATION
INFORMATION SECURITY OFFICE
SECURITY POLICIES AND
INFORMATION TECHNOLOGY PROCEDURES
AUDIT 16 – 09
AUGUST 17, 2016**

/s/ Stephen Mhere

Auditor

/s/ Christine Glover

Audit Director

**TECHNOLOGY AND INNOVATION
INFORMATION SECURITY OFFICE
SECURITY POLICIES AND
INFORMATION TECHNOLOGY PROCEDURES
AUDIT 16 – 09**

BACKGROUND

The Technology and Innovation (T&I) Department's Information Security Office (TISO) was established for the purpose of protecting the City of Tampa (COT)'s information and technology assets, including hardware, software, and data. The key component of COT's effort to protect information assets is the Enterprise Information Security Charter Policy. It was initiated by TISO and COT's executive management to be the foundation of security policies, standards, and procedures. The overall objective of the charter policy is to reduce business and operational risk by maintaining the confidentiality, integrity, and availability of data in networks and other system components.

Headed by the Information Security Officer, TISO has a complement of five members on its staff. The scope of their activities extends beyond protecting information related only to COT employees. TISO is also responsible for protecting COT data processed or accessed by outside contractors, vendors, and individuals who connect to COT networks or otherwise come into contact with COT information assets.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY2016 Audit Agenda. The objectives were to ensure information security policies are documented and that detailed procedures have been developed for areas of critical risk. Based on our review, during the planning stage (see work performed and conclusions below), the audit was concluded and no additional testing was considered necessary.

STATEMENT OF SCOPE

The scope of the audit included enterprise information security policies and procedures for COT. Evidence of implementation of policies and compliance was also included in the audit analysis. This review did not include information security policies and procedures relating to vendors and outside contractors.

STATEMENT OF METHODOLOGY

Audit work involved a review of the following:

- COT's information security policy framework, documentation, and implementation procedures.
- T&I's policy reference manual and security policy manuals of style.
- ISO 27002, a standard of practice for security management that TISO adopted from the International Organization for Standardization (ISO).
- Previous internal audits of T&I for their content on security issues.
- COT personnel policies relevant to information security, disseminated by the Human Resources Department to employees.
- Relevant Florida state statutes.

In addition, we conducted an interview with the director of Technology and Innovation in his capacity as the Chief Information Officer with overall responsibility for information security. Interviews were also conducted with the Information Security Officer whose responsibilities not only include documentation of policies but also their implementation.

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 findings and conclusions based on our audit objectives.

NOTEWORTHY ACCOMPLISHMENTS

Some of TISO's noteworthy accomplishments include the following:

1. Creation of a policy framework mirroring ISO 27002.
2. Development of an information security policy, in conjunction with the Purchasing and Legal Departments, to provide internal controls for COT's use of cloud and offsite hosting services.

AUDIT CONCLUSIONS

Based upon the test work performed, we conclude that COT has effectively documented information security policies and developed procedures that address critical risks. However, COT has not recently performed a comprehensive information security risk assessment.

COMPREHENSIVE SECURITY RISK ASSESSMENT

STATEMENT OF CONDITION: TISO follows international standards, mainly ISO 27002, for information security. ISO 27002 requires that a methodical security risk assessment be completed to help guide and determine appropriate management action and priorities for managing information security risks. The standard also provides that the risk assessment should be repeated periodically to address any changes. However, COT has not recently performed a comprehensive information security risk assessment.

CRITERIA: The adopted ISO 27002 standards require a periodic risk assessment. While ISO 27002 does not define periodic, ISACA¹'s guideline is that comprehensive enterprise security risk assessment should be conducted at least once every two years. NIST² requires all federal agencies to perform the risk assessment process at least once every three years. Currently, the COT is outside of these guidelines for a documented, comprehensive assessment.

CAUSE: T&I has many risk management elements in place: it has identified the most critical information systems, developed detailed procedures for critical policies, regularly conducts network vulnerability assessments, performs appropriate back-up and recovery operations, etc. T&I also has a Continuity of Operations Plan in place. However, TISO is a small office, and has been unable to expand its activities to include a documented comprehensive, city-wide information security risk assessment.

EFFECT OF CONDITION: The primary objective of information security policies is to use them as a basis for internal controls against risks to information technology systems. Without comprehensive and periodic information risk assessments it is difficult to objectively identify risks, making it also difficult to formulate and implement the most appropriate policies.

RECOMMENDATIONS: Within the guidelines of the adopted standards, TISO should revisit and validate their risk assessment processes. These processes should be documented as a comprehensive enterprise information security risk assessment to identify COT's most critical security risks. Considering risks, the assessment should be conducted on an appropriately established periodic basis. The risk assessment results should be used to identify critical areas that may need policies and/or detailed procedures.

MANAGEMENT RESPONSE: Concur. T&I, along with the security office (TISO) does currently identify critical areas that may need policies and/or detailed procedures, primarily accomplished based on current regulatory requirements, institutional knowledge and current threat trends. Yearly we must meet the requirements of the Criminal Justice Information Services (CJIS) Security Policy, The Payment Card Industry Data Security Standard (PCI DSS) and external financial audits. We also actively participate in Wisegate, InfraGard and the Multi-State Information Sharing & Analysis Center (MS-ISAC) to help guide our program to known high-risk threats and business trends.

These requirements address much of the enterprise security risk assessment, but are not contained in a single program and or plan. As such, Management agrees with the recommendations to revisit, validate and document our risk assessment processes.

¹ ISACA (Information Systems Audit & Control Association) is an international professional organization that develops standards for information security, assurance, risk management, and governance.

² NIST (National Institute of Standards and Technology) is a federal technology agency that works with industry to develop and apply technology, measurements, and standards that all federal agencies must comply with.

TARGET IMPLEMENTATION DATE: By 1/30/2017 we will create a plan to cover the following objectives:

- Work with T&I's Enterprise Change Management department to create a divisional outreach program to help TISO engage with our major customers and confirm their security priorities;
- Investigate the concept of integrating governance with the City's Risk Management department as a means of maintaining a lean, effective governance process;
- Create a timeline and coordinate our security and compliance plans and activities with the Internal Audit department so that the scope of activities (like system and application priorities for protection and recovery) are well known, and compliance overlap is reduced while improving effectiveness.

Lastly, because a fully comprehensive enterprise information security risk assessment may include fairly complex enterprise legal, regulatory and acceptable risk requirements currently beyond the current capabilities of TISO, we will seek to validate and expand this multi-year assessment with a comprehensive information security risk assessment performed by a third party in 2017-2018 (scope and budgetary quotes by 12/30/16).