



# CITY OF TAMPA

Bob Buckhorn, Mayor

Internal Audit Department

Christine Glover, Internal Audit Director

July 10, 2015

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

RE: Program Change Control/Problem Management, Audit 15-04

Dear Mayor Buckhorn:

Attached is the Internal Audit Department's report on Program Change Control/Problem Management.

We thank management and staff of Technology and Innovation 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, Chief Technology Officer  
Karl Craig, Change Manager

**TECHNOLOGY AND INNOVATION  
PROGRAM CHANGE CONTROL/  
PROBLEM MANAGEMENT  
AUDIT 15-04  
JULY 10, 2015**

**TECHNOLOGY AND INNOVATION  
PROGRAM CHANGE CONTROL/PROBLEM MANAGEMENT  
AUDIT 15-04  
JULY 10, 2015**

/s/ Stephen Mhere

---

Auditor

/s/ Christine Glover

---

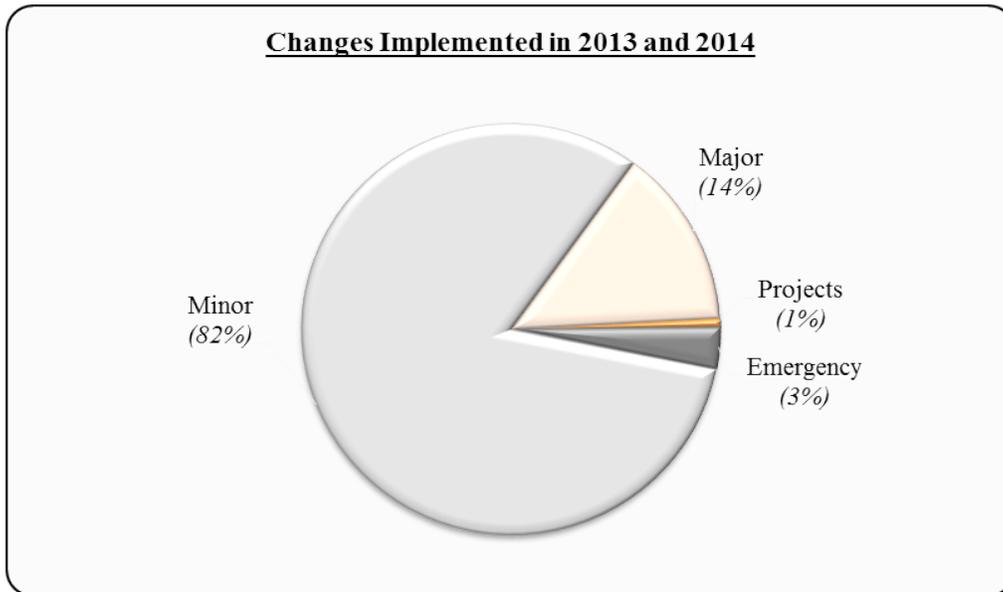
Audit Director

**TECHNOLOGY AND INNOVATION  
PROGRAM CHANGE CONTROL/PROBLEM MANAGEMENT  
AUDIT 15-04**

**BACKGROUND**

Program change control/management is the process of controlling and managing changes introduced in an information technology infrastructure. It ensures efficiency in service operations by standardizing procedures, aids information management by recording all changes to service assets, and promotes business benefit by minimizing the risk of disruption to the production environment. Program change may involve upgrading application software to its newer version, replacing a server, or introducing a new business application for the first time in an organization's operational environment.

The City of Tampa (COT)'s Technology and Innovation Department (T&I) is responsible for program change control and problem management. To accomplish this objective, T&I established a Change Advisory Board (CAB) and charged it with the responsibility to evaluate change requests, assess risks associated with them, and make recommendations to the Chief Information Officer about whether or not to approve them. In 2013 and 2014, COT implemented 707 program changes, five of which were classified as projects, 579 as minor changes, 100 as major, and 23 as emergency changes.



*Source: Auditor analysis of program change records provided by Technology and Innovation Department.*

The process to implement a requested change is dependent upon its classification, i.e., whether it is classified as an emergency change, a project, a major change, or a minor change. The CAB is responsible for triaging all requested changes, based on various classification factors. At the time of this audit, the CAB classified changes according to factors shown in Table 1 below:

**Table 1: T&I's Standard Classification of Requested Changes**

<b>Emergency</b>	Requires immediate action to avert loss of service that may cause major business impact.
<b>Project</b>	Needs more than 160 T&I employee task hours to complete.
<b>Major</b>	Will affect 10 people or more than one city department.
	Has potential for financial or political impact or has potential impact on citizen perception.
	Requires more than one change in more than one element of any system.
	Involves a high business or technical risk based on unproven processes or technologies.
<b>Minor</b>	Will affect less than 10 people or only one department.
	Has no potential for financial or political impact or impact on citizen perception.
	Requires only one change in only one element of any system.
	Involves a low business or technical risk based on using proven processes or technologies.

*Source: T&I documentation of CAB references on Change Types*

### **STATEMENT OF OBJECTIVES**

This audit was conducted in accordance with the Internal Audit Department's FY 2015 Audit Agenda. It had two objectives as described below:

1. To verify that T&I's program change control practices protect the production environment by applying separation of duties principle whereby staff responsible for developing changes do not also have access to the production environment where they can implement unauthorized changes.
2. To verify that changes requested for COT systems are appropriately tested and that test results are satisfactory to end-users before implementation in the production environment.

### **STATEMENT OF SCOPE**

The audit covered calendar years 2013 and 2014, and focused on how T&I executed program change control/problem management functions. Departmental processes, policies, and procedures, as described in standard operating procedures manuals, were reviewed. Contractual agreements for outsourced program change control functions during the audit period were also examined. The audit also covered COT's program change control activities relating to updating of existing business applications, implementation of software acquired from vendors, updating of operating system software, patch management, and upgrading of information technology hardware. A limited evaluation of access controls related to development and migration of programs into the production environment was also performed.

This audit did not include detailed testing of practices utilized during the implementation of software changes in hosted solutions, i.e., production applications software outsourced to contractors/vendors. The reason for this limitation was that T&I did not have control over vendors' change management activities. However, T&I still expected vendors to use industry

best practices in their program change management activities. As such, contractual agreements for outsourced program change control functions were reviewed to determine if they contained language that matched those expectations.

### **STATEMENT OF METHODOLOGY**

The audit reviewed the City of Tampa's program change control policies and procedures, including CAB's charter and standard operating procedures for submitting or updating project requests and creating change records. T&I adopted the Information Technology Infrastructure Library (ITIL) as its standard for providing services to users of information technology. Accordingly, ITIL was also reviewed, as were the COBIT 5 framework and the Federal Information System Controls Audit Manual, which are recognized information technology best practice guidelines for program change control.

Interviews were held with the Chief Information Officer (CIO), a change management project leader, and other T&I staff members with change management responsibilities. They provided their perspectives on the department's performance and its exposure to fraud. The Information Security Officer also provided information regarding the role of his team in change management.

Audit fieldwork involved testing in two critical areas. The first was to evaluate separation of duties practices relating to the development of requested changes and their migration into the production environment. This included a review of compensating controls when such separation does not exist. The second was to evaluate the testing protocols or procedures applied to developed changes prior to their implementation into production.

### **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.

### **AUDIT CONCLUSIONS**

Based upon a review of documented policies and fieldwork, our audit found that T&I has a proper internal control process in place and is effectively and successfully controlling and managing change in the City's information technology infrastructure. Our conclusions were as follows:

1. Program change control practices protect the production environment. In instances where separation of duties between development and migration does not exist, appropriate compensating controls are in place.
2. Changes requested for COT systems are appropriately tested and, end-user feedback on test results is sought.

## **NOTEWORTHY ACCOMPLISHMENTS**

T&I achieved noteworthy accomplishments in its program change control, as described below:

1. In 2013 and 2014 the department achieved a success rate for major change implementation of 95%. By industry best practice standards, a change control program is considered to be successful and well-managed if it attains a major change success rate of 70%.
2. Also, during the same period, T&I used emergency change procedures in 3.3% of all changes it implemented. According to industry best practice standards, a change control program is considered to be well-managed if emergency change procedures are utilized no more than 10% of the time.

While the finding discussed below may not significantly impair T&I operations, it does present a risk that can be more effectively controlled.

## **AUTOMATED DETECTIVE CONTROLS**

**STATEMENT OF CONDITION:** Considering scope, risk, and cost; T&I deploys a number of automated detective controls to monitor and detect changes in the City's information technology operating environment. These tools include network monitoring, security scanning, security firewall, and specific application permissions to transmit on sensitive servers. However, software detective measures could potentially be deployed more extensively, on critical systems, to maximize functionality and benefits.

**CRITERIA:** T&I has adopted, and internal change control policies and procedures reflect, practices described in the Information Technology Infrastructure Library (ITIL). ITIL recommends the use of independent detective controls as a best practice.

**CAUSE:** While T&I has the ability to discover unrecognized applications, currently that capability is not fully realized because the enabling software acquired for auto-detection is not installed in some servers due to licensing compliance requirements. Also, systems for detection of unauthorized modifications to approved applications that are already in use are primarily manual.

**EFFECT OF CONDITION:** Without automated detective software deployed in critical servers the ability to timely identify unrecognized software is diminished. The use of manual discovery methods as the primary means by which to detect unauthorized software modifications also compromises the timeliness of discovering potential problems. As a result, opportunities to minimize disruption of server based services may be reduced.

**RECOMMENDATION:** T&I should consider implementing the following recommendations:

1. Explore a cost-effective licensing strategy that enables deployment of software inventory discovery tool in the most critical production servers then regularly scan those servers to uncover unauthorized or unrecognized software.
2. Implement an automated quarterly inventory process for end-user PC's to ensure compliance with software standards and to identify unlicensed applications.
3. Implement a cost-effective tool that can automatically perform comparisons of file hash values to check for unauthorized modifications of critical applications already being used in the critical production server systems.

**MANAGEMENT RESPONSE:** Management concurs with these observations and is already in the process of investigating and/or acquiring the appropriate software and systems as recommended to address these issues.

**TARGET IMPLEMENTATION DATE:** December 31, 2015.