City and County of San Francisco

Office of the Controller – City Services Auditor

SAN FRANCISCO MUNICIPAL TRANSPORTATION AGENCY:

SFMTA Lacks Effective Controls Over Its Payroll Process and Timekeeping System for Transit Operators

January 31, 2013

OFFICE OF THE CONTROLLER
CITY SERVICES AUDITOR

The City Services Auditor (CSA) was created in the Office of the Controller through an amendment to the Charter of the City and County of San Francisco (City) that was approved by voters in November 2003. Charter Appendix F grants CSA broad authority to:

- Report on the level and effectiveness of San Francisco's public services and benchmark the City to other public agencies and jurisdictions.
- Conduct financial and performance audits of city departments, contractors, and functions to assess efficiency and effectiveness of processes and services.
- Operate a whistleblower hotline and website and investigate reports of waste, fraud, and abuse of city resources.
- Ensure the financial integrity and improve the overall performance and efficiency of city government.

CSA may conduct financial audits, attestation engagements, and performance audits. Financial audits address the financial integrity of both city departments and contractors and provide reasonable assurance about whether financial statements are presented fairly in all material aspects in conformity with generally accepted accounting principles. Attestation engagements examine, review, or perform procedures on a broad range of subjects such as internal controls; compliance with requirements of specified laws, regulations, rules, contracts, or grants; and the reliability of performance measures. Performance audits focus primarily on assessment of city services and processes, providing recommendations to improve department operations.

CSA conducts its audits in accordance with the Government Auditing Standards published by the U.S. Government Accountability Office (GAO). These standards require:

- Independence of audit staff and the audit organization.
- Objectivity of the auditors performing the work.
- Competent staff, including continuing professional education.
- Quality control procedures to provide reasonable assurance of compliance with the auditing standards.

For questions regarding the report, please contact Director of City Audits Tonia Lediju at Tonia.Lediju@sfgov.org or 415-554-5393, or CSA at 415-554-7469.

Audit Team: Elisa Sullivan, Audit Manager
Helen Vo, Auditor-in-Charge
Annie Cheng, Associate Auditor

City and County of San Francisco

Office of the Controller – City Services Auditor

San Francisco Municipal Transportation Agency: SFMTA Lacks Effective Controls Over Its Payroll Process and Timekeeping System for Transit Operators

January 31, 2013

Purpose of the Audit

The audit assessed the effectiveness of the internal controls over the process the San Francisco Municipal Transportation Agency (SFMTA) uses to pay its transit operators. It focused on SFMTA's Trapeze timekeeping system (Trapeze), which is used only for the payroll of transit operators.

Highlights

Because of weak controls over Trapeze, SFMTA's exposure to undue risk of errors or irregularities in transit operator overtime pay is significant. SFMTA paid transit operators more than $148 million in salaries, including more than $25 million in overtime, for fiscal year 2011-12. An estimated 10 percent of the overtime was unscheduled, which occurs when operators are behind schedule and do not complete their transit runs at the scheduled time. Transit operators work under a memorandum of understanding (MOU), the payment provisions of which are built into Trapeze, the scheduling, bidding, dispatching, and timekeeping system used for all transit operators.

The audit found that SFMTA's transit operator payroll process lacks effective controls to ensure that transit operators' unscheduled overtime and other pay types are accurately paid. MOU pay provisions are accurately translated into Trapeze pay codes. However, Trapeze lacks effective information technology controls to ensure system integrity and security. In particular:

- Transit dispatchers do not verify transit operators' unscheduled overtime, and approve this overtime and enter it into Trapeze, which is contrary to the recommended segregation of duties for payroll. Failure to segregate these duties increases the risk of errors or fraud.
- More than 40 percent of unscheduled overtime is not supported by overtime slips, which are completed by transit operators and dispatchers. Many slips lack key information such as the date completed. On some slips, the hours of work indicated do not match the hours recorded in Trapeze.
- SFMTA has not clearly established and documented an MOU implementation process to ensure that all Trapeze changes meet MOU provisions and have been tested.
- SFMTA does not reconcile Trapeze timekeeping data to the City's payroll system to verify accuracy.

Recommendations

The audit report includes 25 recommendations for SFMTA to improve its internal controls over Trapeze and the payroll process. Specifically, SFMTA should:

- Develop and implement procedures to verify and approve unscheduled overtime.
- Segregate the duties of approving and entering overtime hours into Trapeze.
- Thoroughly document all unscheduled overtime on overtime slips and retain the slips in accordance with policy.
- Establish and document a process to change, review, and test MOU provision changes in Trapeze.
- Reconcile Trapeze to the City's payroll system after each pay period.
- Ensure that unqualified transit operators do not receive expert operator premium pay.
- Implement controls to prevent transit operators from receiving birthday pay more than once per year.

Copies of the full report may be obtained at:
Office of the Controller ● City Hall, Room 316 ● 1 Dr. Carlton B. Goodlett Place ● San Francisco, CA 94102 ● 415.554.7500
or on the Internet at http://www.sfgov.org/controller

Highlights (continued)

- A few ineligible operators received expert premium pay and five operators received birthday pay more than once in fiscal year 2011-12.
- Trapeze lacks pay codes to identify time that transit operators work due to special events, which restricts SFMTA's ability to track and possibly recover some of its extra costs.
- SFMTA lacks a sufficiently trained back-up employee who knows enough about Trapeze's functioning to readily address SFMTA business needs. Only one employee makes required changes to Trapeze, and there is no approval process to monitor implemented changes.
- Eleven separated employees still had access to Trapeze, which increases security risks.

Recommendations (continued)

- Establish pay codes in Trapeze to identify costs associated with specific scheduled and unscheduled events.
- Establish and segregate the roles and responsibilities of personnel supporting Trapeze.
- Implement Trapeze's audit trail function for the most critical functions and develop policies and procedures to review, analyze, and retain audit trail logs.
- Terminate the Trapeze access rights of employees who no longer need them.

CITY AND COUNTY OF SAN FRANCISCO
OFFICE OF THE CONTROLLER

Ben Rosenfield
Controller

Monique Zmuda
Deputy Controller

January 31, 2013

Board of Directors
San Francisco Municipal Transportation Agency
1 South Van Ness Avenue, 7th Floor
San Francisco, CA 94103

Mr. Edward D. Reiskin
Director of Transportation
San Francisco Municipal Transportation Agency
1 South Van Ness Avenue, 7th Floor
San Francisco, CA 94103

Dear Board Chairman and Members, and Mr. Reiskin:

The Office of the Controller's City Services Auditor Division (CSA) presents its report of the San Francisco Municipal Transportation Agency (SFMTA) Trapeze timekeeping system (Trapeze) audit. The audit's primary objective was to determine whether SFMTA's internal control structure over the payroll process for transit operators is effective.

The audit concluded that:

- SFMTA's transit operator payroll process lacks effective controls to ensure that unscheduled overtime and other pay types are accurately paid.
- Pay provisions in labor agreements are accurately translated into pay codes in Trapeze.
- SFMTA lacks information technology controls over Trapeze to ensure system integrity and security.

Due to the sensitive nature of one audit finding related to password controls, this report discusses the finding in general terms. CSA is reporting the finding in more detail in a confidential memorandum to SFMTA in an effort to protect Trapeze's security. The audit report includes 25 recommendations for SFMTA to consider. SFMTA's response to the audit is attached as an appendix. CSA will work with SFMTA to follow up on the status of the recommendations made in this report.

CSA appreciates the assistance and cooperation of SFMTA during the audit. For questions, please contact me at Tonia.Lediju@sfgov.org or 415-554-5393, or CSA at 415-554-7469.

Respectfully,

Tonia Lediju
Director of City Audits

cc: Mayor
Board of Supervisors
Civil Grand Jury
Budget Analyst
Public Library

Page intentionally left blank.

TABLE OF CONTENTS

GLOSSARY OF TERMS

Audit trail	Audit trails maintain a history of events made by systems, application processes, and user activity of systems and applications.
BlockBuster	Application module in Trapeze for schedules and runs
board	Board of Directors of the San Francisco Municipal Transportation Agency
City	City and County of San Francisco
CSA	City Services Auditor Division of the Office of the Controller
COBIT	Formerly known as Control Objectives for Information and related Technology (COBIT), a framework for governing and managing enterprise information and technology that supports enterprise executives and management in their definition and achievement of business goals and related information technology goals.
Controller	Office of the Controller
Data integrity	The condition that exists when data is protected from unauthorized, unanticipated, or unintentional modification
Dispatch SOP	Dispatch standard operating procedures, a comprehensive guidebook for division dispatchers
FAMIS	Financial Accounting and Management Information System
FTE	Full-Time Equivalent
FX	Fixed route, an application module in Trapeze for schedules and exceptions
GAO	United States Government Accountability Office
GEAC	A system the City formerly used to calculate employee pay (taken from the former name of a vendor, Geac Computer Corporation)
Generic user account	An information system user account that is not assigned to an individual user
IS	Information systems

IT	Information technology
Logical access control	The process that limits and controls access to an information system to protect against unauthorized system entry or use
MOU	Memorandum of understanding; a contract
NIST	National Institute of Standards and Technology. Documents developed by NIST further its statutory responsibilities under the Federal Information Security Management Act of 2002.
Non-RDO	Not on a regular day off
PeopleSoft	eMerge PeopleSoft is an integrated human capital management system that provides improved human resources, benefits administration, and payroll services to the City's active, retired, and future workforce.
Privileged user account	A system account that authorizes the user to perform security-related functions that ordinary users cannot perform
PPSD	Payroll and Personnel Services Division of the Office of the Controller
Production environment	The system environment that contains live operational data and transactions
RDO	Regular day off
SFMTA	San Francisco Municipal Transportation Agency
SQL	A database language for accessing relational databases such as Oracle.
Trapeze	Trapeze Version 10; the scheduling, bidding, dispatching, and timekeeping system for transit operators

INTRODUCTION

Audit Authority

This audit was conducted under the authority of the Charter of the City and County of San Francisco (City), Section 3.105 and Appendix F, which requires the City Services Auditor Division (CSA) of the Office of the Controller (Controller) to conduct periodic, comprehensive financial and performance audits of city departments, services, and activities.

Background

Established by voter proposition in 1999, SFMTA brought together and oversees the Municipal Railway and the former Department of Parking and Traffic. SFMTA manages and operates the City's network of surface transportation that encompasses pedestrian, bicycles, transit, traffic, and parking. Additionally, SFMTA regulates the taxi industry in San Francisco.

Governance of SFMTA

SFMTA is governed by a seven-member board of directors (board) appointed by the mayor and confirmed by the Board of Supervisors. The board sets policy for SFMTA, approves the budget and appoints the SFMTA's director of transportation who oversees the day-to-day operations of the agency.

The role of transit operators and the Transit Division

Transit operators, employees of the Transit Division of SFMTA, operate a diverse fleet of diesel buses, electric trolley coaches, alternate fuel vehicles, historic streetcars, modern light rail vehicles, and cable cars, providing transit services in the City 24 hours a day, 7 days a week. The mission of the Transit Division is to provide safe, reliable, clean, accessible, and convenient public transportation to any destination in San Francisco. The vehicle fleet is managed at the Transit Division's seven subdivisions. For fiscal year 2011-12, SFMTA had 1,960 budgeted transit operator positions, of which 1,895 were filled as of July 6, 2012. Exhibit 1 shows the breakdown of transit operators in each subdivision of SFMTA's Transit Division.

EXHIBIT 1 Vehicles and Transit Operator Staffing by Subdivision

Subdivision[a]	Transit Vehicle	Budgeted FTE[b] Transit Operators[c]	Actual FTE Transit Operators[d]
Cable Car	Cable Cars	147.5	163.0[e]
Flynn	Diesel Buses – 60 foot	238.0	256.0[e]
Green	Light Rail & Streetcars	321.0	289.0
Kirkland	Diesel Buses – 40 foot	294.0	260.0
Potrero	Electric Trolley Coaches – 40 & 60 foot	331.0	271.0
Presidio	Electric Trolley Coaches – 40 foot	238.0	257.0[e]
Woods	Diesel & Hybrid Buses – 30 & 40 foot	390.0	399.0[e]
Total		1,959.5	1,895.0

Notes:
[a] Excludes the Transit Division's Training subdivision, which employs transit operators in training.
[b] FTE = full-time equivalent
[c] Budgeted staffing is for fiscal year 2011-12.
[d] Actual staffing is as of pay period ending July 6, 2012.
[e] According to SFMTA, due to staffing shifts between subdivisions, actual staffing is higher than budgeted staffing for some divisions.

Source: SFMTA.

The transit operators' current three-year labor agreement started on July 1, 2011.

Transit operators work under a Memorandum of Understanding (MOU) established between SFMTA and the Transport Workers Union of America, Local 250-A. The most recent MOU covers July 1, 2011, through June 30, 2014, and was entered pursuant to interest arbitration on June 13, 2011. The MOU addresses direct pay for services, benefits, and scheduling and hours of work, and is negotiated for the City by the Employee and Labor Relations unit of the Human Resources Division of SFMTA.

The Trapeze system is used for transit operators' payroll.

SFMTA uses the Trapeze Version 10 system (Trapeze), implemented in January 2008, for scheduling, bidding,[1] dispatching, and timekeeping for all transit operators. The City's Time Entry and Scheduling System is used for payroll for all other SFMTA staff. Trapeze timekeeping data is maintained on an Oracle database and has three application modules for users to perform required duties. Trapeze is maintained by the information systems (IS) project director who also works closely with the labor relations unit to ensure that MOU pay provisions are properly translated into Trapeze pay codes so that transit operators are accurately paid.

[1] Transit operators select their runs through a bidding process.

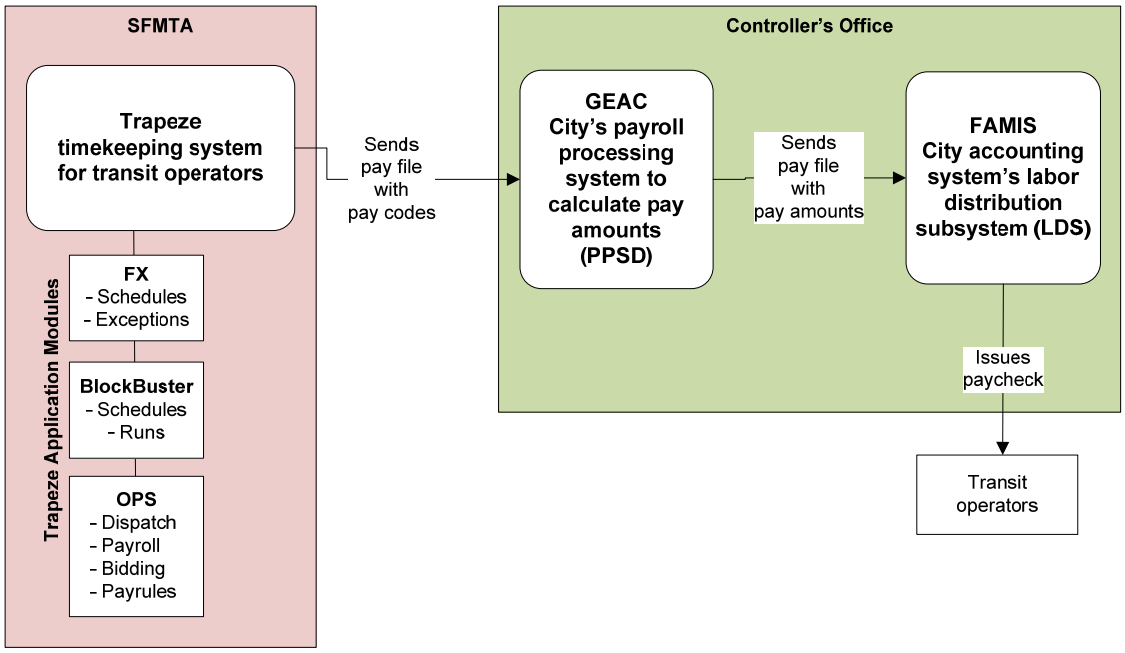
There are three Trapeze environments: one production environment, which contains live operational data and transactions, and two test environments, which contain Trapeze function changes and versions. The test environments allow SFMTA to test, review, and verify the expected results before moving the changes into the production environment. The production environment allows users to perform daily activities and transactions.

Trapeze is interfaced with the Controller's payroll unit for payroll processing.

Every other week, SFMTA's payroll division interfaces and transmits the transit operators' time records from Trapeze to the Controller's Payroll and Personnel Services Division (PPSD) for payroll processing. During the audit period, PPSD processed payroll and personnel data using the GEAC[2] payroll system (GEAC) for employees of all city departments, ensuring compliance with city, state, and federal tax, wage, and hour regulations. Using data from Trapeze, GEAC calculated pay based on the hours worked and applicable tax and payroll deductions. Once payroll was processed, GEAC uploaded the payroll data to the Labor Distribution System, part of the Financial Accounting and Management Information System (FAMIS), the City's financial system. Exhibit 2 shows the high-level system interface between Trapeze and PPSD that existed before August 27, 2012.

[2] GEAC is the former name of a vendor, Geac Computer Corporation.

EXHIBIT 2 **High-Level Interface of Trapeze System Before August 27, 2012**



Source: Auditor analysis of information from SFMTA and Controller.

The City no longer uses GEAC.

In August 2012 PPSD converted its payroll system from GEAC to PeopleSoft 9.0. Trapeze was not changed within SFMTA; however, the interface process was modified to conform to PeopleSoft. CSA did not review the internal controls and processes involved with the conversion from GEAC to PeopleSoft due to the timing of the PeopleSoft conversion.

17 percent of transit operator pay is for overtime.

In fiscal year 2011-12 SFMTA transit operators were paid $148.5 million, including $25.7 million (17 percent) in overtime pay. Exhibit 3 shows the pay by subdivision.

EXHIBIT 3 Transit Operators' Payroll by Subdivision Fiscal Year 2011-12

Subdivision	Total Pay	Unscheduled and Scheduled Overtime Pay	Overtime Pay as % of Total Pay
Cable Car	$15,235,182	$3,863,991	3%
Flynn	18,050,574	2,576,891	2%
Green	25,081,051	5,953,886	4%
Kirkland	20,121,263	2,927,633	2%
Potrero	20,413,506	2,821,614	2%
Presidio	20,391,473	3,873,070	3%
Woods	29,214,467	3,722,823	3%
Total	$148,507,516	$25,739,908	17%

Source: Auditor analysis of Labor Distribution System data.

SFMTA has two categories of overtime, scheduled and unscheduled. Scheduled overtime occurs when overtime is incorporated in a transit operator's run[3] schedule. Unscheduled overtime occurs when transit operators do not complete their runs by the scheduled finish time and must work extra time on a shift. Unscheduled overtime also includes hours when transit operators work on their regular day off (RDO).

Transit operators select their runs through a bidding process.

Three times a year, transit operators use a bidding process to select their run schedule. Trapeze calculates each run's daily pay, factoring in any scheduled overtime or night differential pay. During the bidding process, as transit operators select their runs in order of seniority, union representatives — and, at times, SFMTA scheduling division staff assisting them — enter the transit operators' selected runs into Trapeze. Transit operators' hours and pay are based on the run schedules, except for any unscheduled overtime worked or other exceptions, such as pay for sick leave or vacation, which the subdivision's dispatchers manually enter into Trapeze for each pay period.

Objectives

The objective of this audit was to assess the effectiveness of SFMTA's internal controls over the portion of the timekeeping and payroll process related to Trapeze. Specifically, the audit determined whether:

1. Selected MOU pay provisions are accurately

[3] A run is the route and time of day a transit vehicle operates.

reflected in Trapeze and pay codes in Trapeze adequately cover MOU pay provisions.

2. Pay codes in Trapeze accurately capture all service types (scheduled and unscheduled) and all pay codes are necessary.
3. Transit operators' time entered in Trapeze accurately reflects time worked.
4. Controls over Trapeze are adequate to ensure that changes are authorized and appropriately tested before the payroll is moved to production.

Scope and Methodology

The audit considered Trapeze system data and related documents and policies from January 1, 2008, through September 30, 2012. To conduct the audit, the audit team:

- Reviewed key documents about SFMTA's transit operator and payroll functions, including the MOU between SFMTA and Transport Workers of Union of America, Local 250-A.
- Interviewed SFMTA staff and management personnel to understand controls, procedures, and common practices.
- Obtained and analyzed payroll data from Trapeze and the City's Time Entry and Scheduling System for fiscal year 2011-12.
- Tested 100 percent of unscheduled overtime for three of the seven transit subdivisions for the pay period ending July 6, 2012.
- Assessed whether Trapeze user access privileges are in accordance with business needs.
- Surveyed other jurisdictions for relevant data related to transit operator payroll practices.
- Compared MOU pay provisions to Trapeze pay codes and rates.
- Reviewed selected pay codes in Trapeze for adequacy.
- Tested the accuracy of a sample of premium pay payments to transit operators.
- Analyzed the Trapeze change process, password

control, and limited access control.

Scope Limitation

The audit did not review SFMTA's Trapeze system controls over the interface with the Controller's PPSD PeopleSoft system due to the timing of the PeopleSoft conversion, which was implemented in August 2012.

Statement of Auditing Standards

This performance audit was conducted in accordance with generally accepted government auditing standards. These standards require planning and performing the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. CSA believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

Page intentionally left blank.

CHAPTER 1 – SFMTA Has Weak Controls Over Its Manual Process for Unscheduled Overtime

Summary

SFMTA's transit operator payroll process lacks effective controls to ensure that transit operators' unscheduled overtime is accurately paid. The audit estimates that unscheduled overtime, which is not verified by transit dispatchers, accounted for more than $2.6 million in pay in fiscal year 2011-12. Also, dispatchers both approve and enter into Trapeze transit operators' unscheduled overtime, which are incompatible payroll duties. Best practices dictate that each of these tasks be performed by a separate employee to decrease the risk of errors and fraud.

More than 40 percent of transit operators' unscheduled overtime reviewed was not supported by an overtime slip, and of the slips that the audit reviewed, some were inadequately completed by transit operators and dispatchers. Key approvals such as the signature of the transit operator or dispatcher was missing from many slips and, for one-third of the slips, the hours or date of the overtime noted on the slip did not match the corresponding information in Trapeze.

Finding 1.1

SFMTA does not verify transit operators' unscheduled overtime although it costs an estimated $2.6 million per year.

There is a high risk that SFMTA issues erroneous unscheduled overtime pay because transit operators' non-RDO[4] unscheduled overtime is not verified for accuracy or appropriateness. For the pay period ending July 20, 2012, transit operators reported 2,151 hours of unscheduled overtime, corresponding to pay of $89,608, or 10 percent of total overtime paid.

Exhibit 4 shows amounts paid for scheduled and unscheduled overtime, including an adjustment for RDO

[4] Non-RDO unscheduled overtime occurs when transit operators do not complete their runs by the scheduled finish time and must work extra time on a shift. "Non-RDO" means the overtime did not occur on the transit operator's regular day off.

overtime, for the pay period ending July 20, 2012.

EXHIBIT 4 Transit Operators' Scheduled and Unscheduled Overtime Pay by Subdivision: July 7 Through July 20, 2012

Sub-division	Total Overtime Pay	Scheduled Overtime Pay	Scheduled as % of Total	Unscheduled Overtime Pay	Regular Day Off (RDO)*	Adjusted Unscheduled Overtime Pay	Adjusted Unscheduled as % of Total
Cable Car	$150,589	$87,089	58%	$63,501	$45,423	$18,077	12%
Flynn	87,885	76,155	87%	11,730	15,314	(3,584)	(4%)
Green	232,273	118,977	51%	113,297	76,015	37,282	16%
Kirkland	100,662	81,930	81%	18,732	17,712	1,020	1%
Potrero	102,980	64,154	62%	38,826	31,097	7,729	8%
Presidio	133,898	94,524	71%	39,374	26,347	13,027	10%
Woods	125,144	76,360	61%	48,784	32,726	16,057	13%
Total	$933,431	$599,189	64%	$334,244	$244,634	$89,608	10%

*Note: There should be fewer RDO overtime hours than unscheduled overtime hours because RDO overtime is recorded as part of unscheduled overtime. However, according to SFMTA, due to a pay code mapping[5] error, this is not always the case.

Source: Auditor analysis of Labor Distribution System data.

Since SFMTA did not track scheduled and unscheduled overtime separately until July 2012, no such figures are available from SFMTA for earlier periods. However, the pay period the audit analyzed indicates that unscheduled overtime is approximately 10 percent of total overtime. If the sample pay period is representative, unverified overtime of 10 percent, or $2.6 million, of the $25.7 million in overtime paid in fiscal year 2011-12[6] is a significant amount of pay.

According to SFMTA, to indicate their overtime hours, transit operators must complete a Transit Operator Vehicle Log, otherwise known as an unscheduled overtime slip, and submit it to a dispatcher. Dispatchers are tasked with reviewing, approving, and entering unscheduled overtime into Trapeze. However, dispatchers are not required to — and do not — verify the unscheduled overtime worked.

According to SFMTA, transit operators are required to call SFMTA's Central Control during their runs if they are

[5] The pay codes in Trapeze are mapped to the City's payroll codes for payroll processing.

[6] Exhibit 3 shows the total pay and overtime pay by subdivision for fiscal year 2011-12.

running behind schedule. According to Central Control, it does not log the instances when transit operators are simply running late. Central Control only logs instance of accidents or incidents that occur on the vehicles. Conversely, SFMTA lacks a process in place at the dispatch level to notice the dispatchers of overtime incurred by the transit operator. As a result, there is no verification of transit operators' unscheduled overtime.

According to the United States Government Accountability Office (GAO), supervisors have primary responsibility for authorizing and approving time entries, including in exception-based timekeeping systems. Also, time entries should be verified. Organizations often require that timesheets be approved and signed by a supervisor.[7]

A June 2012 report by the National Center for Transit Research addresses best practices, standard operating procedures and uses of technology in dispatch for small, medium, and large transit agencies in Florida. The report noted positive impacts on dispatch functions by new technologies such as new communications systems, computer-aided dispatch, and automated vehicle location packages.

Recommendations

SFMTA should:

1. Develop and implement procedures in which supervisors verify for accuracy and approve unscheduled overtime.

2. Review and assess the feasibility of adopting new technologies such as new communications systems, computer-aided dispatch, and automated vehicle location packages to allow SFMTA to better manage overtime, with the aim of reducing unscheduled overtime.

Finding 1.2

SFMTA lacks segregation of duties in reviewing, approving, and entering transit operators' unscheduled overtime.

[7] Syracuse University, Audit and Management Advisory Services, *Internal Controls for Payroll*, 2012.

Each SFMTA dispatcher must review, approve, and enter into Trapeze transit operators' unscheduled overtime, which is contrary to best practices for segregation of payroll duties. An employee who reviews and approves overtime should not have the authority to enter unscheduled overtime into a timekeeping system. Failure to segregate these duties increases the risk of errors or fraud occurring and of such errors not being detected promptly.

According to four subdivision superintendents interviewed, they are not involved in the day-to-day time entry or review and approval of unscheduled overtime. Superintendents oversee operations to ensure that transit operators follow rules and vehicles start their runs according to schedule. Additionally, superintendents handle any violations reported from street inspectors, accident reports, complaints, and disciplinary issues.

According to the GAO, supervisors have primary responsibility for authorizing and approving time entries, including in exception-based timekeeping systems. And according a published report[8], potentially incompatible duties exist if an individual performs duties in more than one category, such as approval and recording, or if an individual is responsible for performing a control over the same transaction that the individual is responsible for recording.

Recommendation

3. SFMTA should develop and implement procedures in which the employee who verifies and approves unscheduled overtime does not also enter these hours in Trapeze.

Finding 1.3

More than 40 percent of unscheduled overtime was not supported by overtime slips, which corresponds to estimated pay of $1.1 million.

More than 40 percent of unscheduled overtime is not supported by overtime slips.

Forty-four percent of transit operators' unscheduled overtime was not supported by overtime slips. The audit reviewed all unscheduled overtime at three of SFMTA's seven transit divisions for the pay period ending July 6, 2012, and could not verify over 1,000 instances in

[8] IT Governance Institute, *IT [Information Technology] Control Objectives for Sarbanes-Oxley*, 2006

unscheduled overtime. Without adequate supporting documentation for unscheduled overtime, SFMTA increases the risk that paid overtime is inaccurate or fraudulent. If the sample pay period reviewed is representative, then 44 percent of $2.6 million — the total unscheduled overtime estimated in Finding 1.1 — would amount to approximately $1.1 million, a significant amount of unsupported overtime pay. Because management does not verify unscheduled overtime and does not appear to emphasize the need to submit overtime slips, transit operators may perceive that the requirement is not enforced. The amount of unsupported, unscheduled overtime at the three divisions reviewed is shown in Exhibit 5.

EXHIBIT 5 **Unscheduled Overtime of Transit Operators June 23 Through July 6, 2012**

Subdivision	Unscheduled Overtime Instances	Unsupported Unscheduled Overtime Instances	Less RDO Overtime Instances	Adjusted Unsupported Unscheduled Overtime Instances	Unsupported Instances as % of All Unscheduled Overtime Instances
Green	1,273	864	225	639	50%
Kirkland	531	211	12	199	37%
Potrero	644	338	97	241	37%
Total	2,448	1,413	334	1,079	44%

Source: CSA test results.

According to dispatchers at the Green and Potrero subdivisions, they do not always get overtime slips from transit operators for unscheduled overtime. In some cases, a transit operator tells the dispatcher of the unscheduled overtime and the dispatcher enters the time into Trapeze without requiring an overtime slip. The Potrero subdivision's practice is to discard the overtime slips after several pay periods if no complaints or inquiries are made about the overtime.

According to SFMTA's dispatch standard operating procedures (Dispatch SOP), the unscheduled overtime card is an official payroll document that operators must complete. Transit operators must take the cards to a dispatcher for time entry; transit operators may not communicate the time that they worked to the dispatcher

by phone.

According to the San Francisco Ethics Commission's records management policy, city departments are to retain payroll records for two years and get permission from the San Francisco Employees' Retirement System before destroying them. Additionally, although SFMTA's *Record Retention and Destruction Schedule* manual for the Payroll Division does not specifically list overtime slips, it does state that payroll documents (i.e., timesheets) are to be retained for seven years.

Recommendations

SFMTA should:

4. Enforce its procedures to require that all unscheduled overtime is documented on an overtime slip.

5. Ensure that all overtime slips are retained in accordance with SFMTA's record retention policy.

Finding 1.4

Transit operators and dispatchers did not adequately complete overtime slips.

Some unscheduled overtime slips lacked key required information.

Of the unscheduled, non-RDO overtime slips that were available for review from the Kirkland, Green, and Potrero subdivisions for the pay period ending July 6, 2012, some lacked either a transit operator's signature or a dispatcher's signature, or the date and hours on the slip did not reconcile to the Trapeze timekeeping summary.

Exhibit 6 characterizes the information missing from unscheduled overtime slips.

EXHIBIT 6 **Information Missing From Transit Operators' Unscheduled Overtime Slips June 23 Through July 6, 2012**

Subdivision	Total Overtime Slips Available for Review	Slip Not Signed by Transit Operator		Slip Not Signed by Dispatcher		Date/Hours on Overtime Slip Do Not Match Trapeze	
Green	409	3	1%	116	28%	95	23%
Kirkland	320	4	1%	107	33%	115	36%
Potrero	409	105	26%	106	26%	173	42%
Totals	1,138	112	10%	329	29%	383	34%

Source: CSA fieldwork test results.

Without adequate information on the supporting documents (slips) and/or failure to submit required slips, there is no way to determine whether the unscheduled overtime paid is accurate. Because management does not appear to emphasize the need to fully complete overtime slips, transit operators may perceive that the requirement is not enforced, and this could lead to an increased risk of unidentified errors or fraudulent unscheduled overtime claims.

Unscheduled overtime paid in Trapeze does not agree to supporting overtime slips more than one-third of the time.

Of the results shown in Exhibit 6, the most alarming is that 34 percent of the time the data dispatchers entered in Trapeze did not match the date and/or time information on the transit operators' overtime slips. For example:

- A slip indicated that overtime was worked on June 6, 2012, but the Trapeze report showed the overtime was worked on July 5, 2012.
- A slip indicated 23 minutes of overtime worked, but the Trapeze report showed 37 minutes of overtime recorded.
- A slip indicated 2 hours and 3 minutes of overtime worked, but the Trapeze report showed 1 hour and 22 minutes of overtime recorded.
- Some slips lacked a date or the overtime hours worked.

These discrepancies may indicate that dispatchers are not careful to ensure correct time entry or they are intentionally changing the documented hours.

Payroll clerks may spot-

According to SFMTA, payroll clerks in the Payroll

check reported unscheduled overtime but are not in a position to know whether it is correct.

Division spot-check unscheduled overtime. However, payroll clerks are not verifying for accuracy. Further, as discussed earlier, supervisors do not verify overtime worked so they cannot detect unscheduled overtime discrepancies.

According to dispatchers, when transit operators believe an underpayment has occurred for their unscheduled overtime, they will bring this to the dispatcher's attention and fill out a payroll correction request form. The division superintendent reviews the overtime adjustment on the payroll correction request form to the overtime slips and approves the adjustment. However, if an overtime slip was not submitted or lacks required information, then the superintendent cannot verify the underpayment. Besides, relying on transit operators to review the unscheduled overtime pay on their paychecks is not an acceptable or reliable control to detect overpayments for unscheduled overtime.

According to the Dispatch SOP, unscheduled overtime cards are an official payroll document and must be filled out by the operators. The Dispatch SOP does not address that overtime slips must be adequately completed with date, overtime hours worked, and signatures from the transit operator and supervisor.

Recommendations

SFMTA should:

6. Add specific overtime slip completion requirements for transit operators in the dispatch standard operating procedures.

7. Establish a procedure to ensure that all unscheduled overtime slips are adequately completed and submitted. The procedure should include that dispatchers will reject and return to transit operators insufficiently or incorrectly completed slips. The procedure should also include a periodic internal audit process of checking slips for existence and accuracy.

8. Periodically train all dispatchers to follow standard time-entry procedures and, as part of exception-based time-entry, to spot specific anomalies in transit operators' reported hours.

CHAPTER 2 – SFMTA Lacks Effective Controls Over Its Transit Payroll Process

Summary

SFMTA lacks effective controls over its transit payroll process to ensure and verify that transit operators are accurately paid. SFMTA lacks a process to ensure that pay provisions in the transit operators' memorandum of understanding (MOU) are accurately translated into Trapeze pay codes, are successfully tested, and are approved by appropriate personnel, such as labor relations management. Trapeze is a mission-critical system, as SFMTA used Trapeze to record hours equivalent to almost $150 million in pay to about 1,900 transit operators during fiscal year 2011-12. Errors in the system could be costly and result in inaccurate payroll that needlessly requires staff time to fix.

SFMTA does not reconcile Trapeze timekeeping data to the City's payroll system to verify accuracy, and lacks a comprehensive payroll policies and procedures manual. Further, obsolete and irrelevant pay codes have not been deleted from Trapeze, and Trapeze lacks configured pay codes to identify special events, which restricts SFMTA's ability to potentially recover costs associated with those events and to accurately report those costs to policymakers. Last, Trapeze lacks a system control to prevent transit operators from receiving birthday pay more than once per year.

Finding 2.1

SFMTA has not clearly established and documented the MOU implementation process to ensure that Trapeze changes meet all MOU provisions and have been tested.

SFMTA updated Trapeze based on the 2011 MOU's pay provisions but did not update the system "crosswalk" documentation accordingly.[9] SFMTA also does no independent review, approval, or testing of the changes in Trapeze associated with changes to the MOU provisions. Without the crosswalk documentation and

[9] The crosswalk identifies MOU provisions and links them to the associated pay rules in Trapeze used to implement the provisions.

proper change-control procedures, SFMTA cannot be assured that all Trapeze changes completely meet all MOU provisions and have been tested to ensure that the changes are correct.

According to SFMTA management, when Trapeze was implemented in 2008, the MOU pay provisions were compared to the Trapeze pay rules and the documentation was "crosswalked" to the system. However, when the MOU was updated in 2011, only four provisions required changes to Trapeze. The changes were made but not documented in the crosswalk. According to SFMTA management, the IS project director is responsible for implementing MOU provision changes in Trapeze, but no review or approval process to ensure accuracy exists.

COBIT 5 recommends that changes to the system should be tracked to requirements, enabling all stakeholders to monitor, review, and approve the changes and to ensure that all stakeholders and the business process owner fully understand and agree on the outcomes of the changes.[10]

Recommendation

9. SFMTA should establish and document a formal process to ensure that any change to the Trapeze system related to the transit operators' memorandum of understanding be:
    - Clearly documented at the time of the change.
    - Independently reviewed, approved, and tested before it is implemented.

Finding 2.2

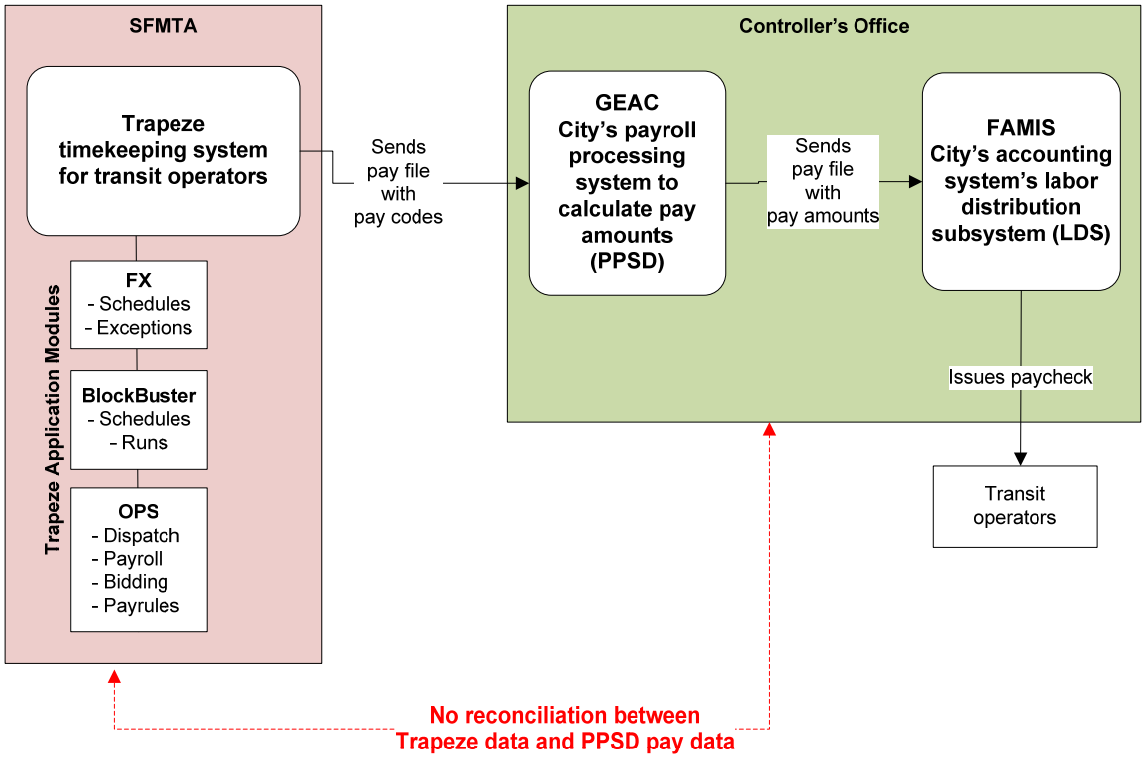
SFMTA does not reconcile Trapeze timekeeping data to City payroll system data.

SFMTA does not reconcile timekeeping data in Trapeze to the Controller's payroll data that documents what is actually paid. Such a reconciliation would ensure that the data transmitted by SFMTA and payroll paid by the Controller to transit operators is complete, accurate, and valid.

[10] COBIT 5, the current version of COBIT, is a complete, internationally accepted framework for governing and managing enterprise information and technology.

SFMTA transit operators' timekeeping data is transferred from Trapeze through an interface file to the Controller's PPSD for payroll processing. Once the payroll is paid, SFMTA does not verify that the hours paid to transit operators match those in Trapeze. Lack of reconciliation between the two systems prevents SFMTA from identifying possible errors in transit operator pay. Exhibit 7 illustrates the reconciliation controls missing from the payroll process used for transit operators.

EXHIBIT 7 **High-Level Interface of Trapeze System Before August 27, 2012**



Source: Auditor analysis of information from SFMTA and Controller.

Data in the Trapeze and PPSD payroll systems differ, and the causes of the differences are unknown.

The audit attempted to reconcile timekeeping and payroll data between Trapeze and PPSD's payroll system for fiscal year 2011-12, and found discrepancies in the total number of employees and total number of hours reported, as follows.

- **Total transit operators**: PPSD's payroll system shows 18 more transit operators than Trapeze.

- **Total hours**: Trapeze shows 1.23 million more hours than PPSD's payroll system.[11]

According to SFMTA management, numerous factors could explain the variances, such as Trapeze reporting only hours worked and excluding employees on long-term leave. However, due to the difficulty and time that would be needed to thoroughly review the details, neither SFMTA nor the audit attempted to determine the cause for the differences. According to SFMTA management, reconciliations of data in the two systems have never been performed but should be performed regularly. Moreover, SFMTA plans to implement reconciliation procedures now that PPSD has completed the conversion to the new PeopleSoft payroll system.

According to the GAO's Joint Financial Management Improvement Program, organizations must provide for reconciliations of data in their payroll systems to data in their disbursing, accounting, and other administrative systems to ensure accuracy, completeness, and data integrity.

Recommendation

10. SFMTA should develop and implement procedures to consistently reconcile data in the Trapeze system to data in PPSD's payroll system after each pay period. A supervisor should review and approve the reconciliations.

Finding 2.3 **Ineligible transit operators received expert premium pay.**

SFMTA overpaid expert operator premium pay to at least 13 employees.

Thirteen transit operators with 560 reported work hours in the pay periods the audit tested in detail (January 21 through July 6, 2012) received expert operator premium pay although they were not on the list of those qualified to receive it, resulting in an overpayment of at least $280.

According to the MOU, transit operators are eligible for an expert operator premium of $0.50 per hour if they meet certain conditions, such as having worked five consecutive years at one location or driven at least 1,600

[11] Difference between audit's analysis of the total number of hours in the Labor Distribution System (a PPSD system) and Trapeze transmittal files for fiscal year 2011-12.

hours in the previous fiscal year. Every year, SFMTA reviews each transit operator's status and produces a list of transit operators qualified to receive the expert operator premium. The list is given to SFMTA's Information Technology (IT) division, to update the status of transit operators in Trapeze so they can receive the premium. According to SFMTA management, these 13 transit operators received expert operator premium pay (and had expert operator status in Trapeze) although they are not on the eligibility list because of Trapeze user entry errors. This occurred because certain Trapeze users have system access that allows them to change transit operators' premium pay status. However, due to limitations in Trapeze access security, it may be impossible to restrict user access further in the current version of Trapeze.

Recommendations

SFMTA should:

11. Immediately change (to ineligible) the status in the Trapeze system of all transit operators identified as eligible to receive expert operator premium pay that are not on the list of those qualified for this pay.

12. Establish procedures to periodically review Trapeze system-generated reports on employees' pay status and pay status changes to ensure that all premium pays, including expert operator premium pay, are appropriately applied.

Finding 2.4

More than once, five transit operators received birthday pay in fiscal year 2011-12.

SFMTA overpaid $1,181 in birthday pay in fiscal year 2011-12.

Five transit operators received birthday (holiday) pay more than once during fiscal year 2011-12, resulting in 40 hours or $1,181 overpayment by SFMTA. Before July 1, 2012, Trapeze did not have sufficient automated processing controls to prevent this user error. Lack of system controls over birthday pay increases the risk that transit operator birthday pay is incorrect.

According to the MOU, transit operators' birthdays are to be considered holidays and, therefore, are to be paid as such once a year. However, before July 1, 2012, Trapeze did not have an automated control to prevent

dispatchers from entering birthday pay more than once per year per employee.

Recommendation

13. SFMTA should ensure that Trapeze system controls prevent transit operators from receiving birthday pay more than once per year.

Finding 2.5

Because Trapeze pay codes are not configured to identify special events, SFMTA cannot account for or recover some of its extra costs.

Costs associated with special events cannot be identified in Trapeze, so cannot be analyzed or recovered.

In fiscal year 2011-12 Trapeze pay codes were not configured to identify hours worked due to scheduled or unscheduled special events.[12] Thus, SFMTA does not know the labor costs associated with special events and is unable to recover extra labor costs for which outside parties may be responsible. Moreover, SFMTA cannot even report these special event costs to policymakers.

Although SMFTA may be unable to recover all such costs from outside parties even if it could identify them, it makes good business sense for it to identify and categorize its payroll costs associated with special events for reporting purposes. At a minimum, quantifying these costs could assist SFMTA management and city decision makers in understanding and managing costs including transit operator overtime. According to SFMTA management, special index codes are being implemented for fiscal year 2012-13.

Recommendation

14. SFMTA should continue to establish index codes to identify the costs associated with specific scheduled and generic unscheduled special events. In doing so, SFMTA should identify specific recurring and one-time scheduled events whose sponsors SFMTA may be able to bill to reimburse it for the extra costs it incurs, including transit operator overtime, to provide transit service.

[12] Scheduled special events for which SFMTA provides extra transit service — or that disrupt transit service due to street closures — include some large outdoor concerts and festivals, street fairs, and athletic and sporting events. Unscheduled special events that can disrupt SFMTA transit service and may require extra transit operator hours include traffic accidents, fires, demonstrations, and other events that cause street closures.

Finding 2.6 **SFMTA does not deactivate obsolete pay codes in Trapeze.**

Of the 48 pay codes in Trapeze, 12 (25 percent) were not used in fiscal year 2011-12 and do not have the corresponding active pay rules in Trapeze that are needed to process payroll accurately. Therefore, these pay codes are obsolete. Not deactivating unused pay codes increases the risk of them being used by dispatchers or payroll staff, which could result in inaccurate calculation of transit operators' pay.

According to SFMTA management, SFMTA has no defined process to review and deactivate unused pay codes and pay rules when they become irrelevant. Pay codes are continually added to Trapeze to accommodate necessary changes, but pay codes are not deactivated. Pay codes cannot be deleted from Trapeze because they are still associated with prior payroll, but obsolete pay codes can be deactivated to exclude them from future use.

According to COBIT 5, organizations should implement controls to measure the use and evaluate the currency and relevance of information, and retire obsolete information.

Recommendation

15. SFMTA should periodically reassess the need for each pay code in Trapeze and deactivate obsolete pay codes.

Finding 2.7 **SFMTA lacks a comprehensive policies and procedures manual for its payroll processing.**

SFMTA has no complete policies and procedures manual for its payroll process. SFMTA has some procedure documents specific to Trapeze, such as the Dispatch SOP and Trapeze user guides for each of the Trapeze modules, such as Fixed Route (FX) and BlockBuster. SFMTA also has agency-wide written procedures on various payroll topics, such as a "Timekeeping Cheat Sheet" and Equal Employment Opportunity Hiring Policy and Procedure. However, there is no single comprehensive document that contains all payroll policies and procedures, including for transit

operators' payroll.

Without a comprehensive payroll policies and procedures manual, payroll process controls may be inconsistent among payroll staff throughout the organization. SFMTA management acknowledged that the agency lacks a comprehensive payroll policies and procedures manual, and explained that, because PPSD has converted its payroll to the new PeopleSoft system, SFMTA will be drafting new policies and procedures. Once the new policies and procedures are completed by PPSD, SFMTA will develop agency payroll policies and procedures in accordance with PPSD's.

According to GAO Standards for Internal Controls, appropriate documentation of transactions and internal controls should be in administrative policies or operating manuals, and all documentation should be properly managed and maintained.

Recommendation

16. SFMTA should develop a single, comprehensive, up-to-date policies and procedures manual for its payroll process that is in accordance with citywide payroll procedures.

CHAPTER 3 – SFMTA Lacks Effective Information Technology Controls to Ensure System Integrity and Security Over Its Trapeze System

Summary

Trapeze lacks effective information technology controls to ensure system integrity and security. The fact that one employee, the IS project director, fully controls the day-to-day operations and maintenance of Trapeze increases the risk of errors and the possibility of undetected compromises of the system. In addition, SFMTA has no method to ensure that all system changes to Trapeze are properly documented, approved and tested because Trapeze cannot generate a complete and accurate inventory of all changes made to the system. Although SFMTA has IT change management policies and procedures, it does not regularly review and update them and does not always adhere to them. The audit also found that 11 separated employees still had access to Trapeze, and generic test accounts existed in the Trapeze production environment, increasing security risks. Finally, Trapeze's password controls do not meet industry standards intended to reduce the risk of unauthorized access.

Finding 3.1

SFMTA lacks a sufficiently trained back-up employee who knows enough about Trapeze's functional aspects[13] to readily address SFMTA business needs.

One employee has full access to the payroll module, has no sufficient back-up, and can make changes in Trapeze without adequate testing, review, and approval.

Although SFMTA's IT personnel have full access to support technical[14] system issues, the bulk of the functional duties lie with the IS project director, who is responsible for the day-to-day functional support, operations, and maintenance of Trapeze. This is a problem for two reasons:

- SFMTA is not fully prepared for the absence of the IS project director, which impedes its ability to

[13] Functional aspects of an application involve changes in calculations, data manipulations, processing, and other functionality that affects what the application is supposed to accomplish based on business requirements.

[14] Technical system support involves the server, operating system, database, and files that allow systems to interface.

execute a critical business function. SFMTA lacks a sufficiently trained back-up employee to handle the day-to-day needs of Trapeze, other than executing the biweekly payroll. Thus, these critical needs may not be adequately or promptly attended to when the IS project director is absent. Further, SFMTA would find it difficult to train another employee to take on these duties if the IS project director were to leave suddenly or no longer have these assigned duties.

- By assigning Trapeze duties to one employee and providing no oversight, SFMTA is highly susceptible to risk of errors or fraud and does not meet IT industry practice standards of segregation of duties. The IS project director has excessive access to and control of Trapeze. This access allows the IS project director to make changes without adequate testing, review, and approval. Although the audit did not uncover any fraudulent activity, the current arrangement poses an unacceptable risk that one employee could compromise the payroll process or data without detection.

Segregation of duties is a widely accepted internal control that entails distributing key duties among different people, reducing the possibility that anyone could compromise a critical process and adversely affect the integrity of data. According to COBIT 5, establishing and defining roles and responsibilities, having back-up staff, and cross-training requirements are important criteria for IT service continuity. Further, COBIT 5 provides guidance on allocating roles for sensitive activities with clear segregation of duties and regularly making employees aware so that everyone understands their responsibilities, the importance of controls, and the integrity of information.

Recommendation

17. SFMTA should establish and segregate the roles and responsibilities of personnel supporting Trapeze. These roles must clearly reflect SFMTA's overall business needs and information technology objectives and ensure sufficient back-up support and cross-training to reduce the risk of major disruption to Trapeze system operations.

Finding 3.2 **SFMTA does not maintain effective change management controls in the Trapeze production environment.**

There was no evidence that all changes were approved and tested.

According to SFMTA management, Trapeze cannot generate a complete and accurate inventory of all changes made to the functionality of the system as required by COBIT, thus, enabling ad hoc changes to Trapeze without formal documentation, testing, review, and approval by key stakeholders. The lack of "time stamp" information and maintenance of complete and accurate inventory of all critical changes such as a pay rule or pay code change in Trapeze makes it impossible to identify when and who made the change. Although the audit found no major problems in this regard, SFMTA has no method to ensure that all changes are properly approved and tested.

For example, the audit discovered that Trapeze did not have the required birthday pay rule to prevent birthday pay from being awarded to the same employee more than once a year, as discussed in Chapter 2. When this observation was discussed with the IS project director, immediately a rule was activated in the production environment without proper documentation, review, and approval. In addition, the audit's analysis of unscheduled overtime discussed in Chapter 1 resulted in SFMTA researching and discovering a Trapeze mapping error that had previously gone undetected. Further, the IS project director acknowledged that SQL[15] update statements sometimes are made directly to the database, resulting in an undocumented time stamp of the last update for some pay rule changes.

The audit trail feature in Trapeze is not used.

According to SFMTA management, Trapeze and its related Oracle database have an available audit trail feature that SFMTA has not turned on to avoid potential performance problems. Without adequate audit trail and change management controls — such as documentation, testing, review, and approval — in Trapeze, SFMTA runs an undue risk of unauthorized system and functional changes that could degrade the integrity of the data and

[15] SQL is a database language for accessing relational databases such as Oracle.

application, resulting in inaccurate pay.

According to COBIT 5, all change requests should be evaluated to determine the impact of business processes and IT services, and to assess whether changes will adversely affect the operational environment and introduce unacceptable risk. Changes should be planned, categorized, prioritized, scheduled, and authorized before they are made, and logged and assessed after they are made.

The National Institute of Standards and Technology states that it is critical to maintain an accurate inventory of all changes to an information system.[16]

Recommendations

SFMTA should:

18. Review and formally determine which transactions and system changes in Trapeze and its related Oracle database are most critical. Apply the audit trail functionality to the most critical transactions and changes if this can be done without significantly degrading system performance.

19. Develop policies and procedures to review, analyze, and retain audit trail logs.

20. Ensure that all system changes in Trapeze and its related Oracle database are tested and approved by appropriate SFMTA personnel.

Finding 3.3

SFMTA does not regularly update, and does not always follow, its information technology change management policies and procedures.

Although SFMTA has IT change management policies and procedures, it does not regularly review and update them, so they may not reflect current, intended practices. The IS project director also does not always adhere to the IT change management policies and procedures, sometimes making ad hoc changes without formal approval by the change control committee. Further,

[16] NIST, *Security Considerations in the Information System Development Life Cycle*, special publication 800-64 (SP800-64), revision 2, 2008. This guide focuses on the information security components of the system development life cycle.

SFMTA's change policies and procedures do not define the consequences for noncompliance. Without well-developed, adopted, and disseminated policies and procedures for its staff to adhere to, there is greater risk of inconsistencies and errors being undetected or changes performed that do not meet SFMTA's business requirements.

According to COBIT 5, IT policies should be evaluated and updated at least yearly to accommodate changing operating or business environments. In addition, procedures should exist to track compliance with policies and define the consequences of noncompliance.

Recommendation

21. SFMTA should update its information technology change management policies and procedures, at minimum annually, to reflect current practices and to meet SFMTA's business objectives. Additionally, the policies and procedures should be approved and communicated to all staff.

Finding 3.4

Separated employee user accounts and generic accounts exist in the Trapeze production environment.

Some separated employees still have access to Trapeze.

Because SFMTA lacks effective logical access controls,[17] some separated employees still have access to Trapeze, as follows:

- Ten separated transit operators and dispatchers still have access to Trapeze.
- One separated IT employee has administrator access in Trapeze.
- Two generic test accounts exist in the production environment.

The presence of generic test accounts in a production environment could pose a security risk because these accounts are shared among IT application team members. This procedure results in several people knowing the login username and password for these test accounts, which makes it more difficult to identify which

[17] Logical access controls are the system-based mechanism used to specify who or what is to have access to a specific system resource and the type of access that is permitted.

individual performed an activity in the system.

Although access to Trapeze requires users to first login successfully to SFMTA's network, the failure to disable application access for separated employees can increase the risk of employees inappropriately accessing Trapeze. Weaknesses in user account management can lead to employees having unnecessary and inappropriate access that compromises the integrity of Trapeze and its data.

SFMTA management acknowledged there is only ad hoc review, not a formal process, for assessing and, when necessary, closing Trapeze user accounts. Such a process must be done periodically to confirm that only authorized individuals have access to Trapeze. According to SFMTA management, each month a system-generated report from SFMTA's Human Resources Division is reviewed and system access of all separated employees is disabled. However, this process cannot detect other system users — for example, employees who have changed job classifications — whose access should be terminated. No one, neither the IS project director nor IT application manager, reviews access rights of Trapeze user and administrative accounts to ensure that access is appropriate.

According to COBIT 5, an organization should have controls to address administration of all logical access changes (creation, modifications, and deletions) of user and privileged user accounts.[18] Controls should also include ones to ensure that all users are uniquely identifiable and a regular management review of all accounts and related privileges is conducted.

Recommendations

SFMTA should:

22. Review the current security profiles for all Trapeze users and administrators and ensure that the system access rights of employees who no longer need this access are immediately terminated.

23. Establish written procedures and a schedule for

[18] A privileged user is authorized to perform security-related functions that ordinary users are not authorized to perform.

periodically reviewing user lists and the associated access rights for Trapeze.

24. Review and assess generic Trapeze accounts to determine if they are necessary and, if so, whether users' access levels are adequately limited. Disable unnecessary generic accounts and reduce unnecessary access levels.

Finding 3.5 **Password controls in Trapeze can be improved to enhance system security.**

Due to the confidential nature of this finding, the complete finding is not included here. CSA has provided SFMTA with a memorandum of the full details of this finding.

SFMTA does not require Trapeze users' passwords to meet certain requirements that would enhance password security.

Without a well-developed, adopted, and disseminated enterprise-wide password policy for Trapeze users to adhere to, SFMTA creates an undue risk of unauthorized access to Trapeze being undetected and, therefore, increases the risk of jeopardizing the integrity of data in the system.

According to SFMTA management, employees would have difficulty remembering their passwords if they were forced to change them periodically, which would cause the IT group to be contacted frequently with password reset requests.

A guide for California counties[19] recommends that strong passwords should:

- Contain both upper and lower case characters (i.e., A-Z and a-z).
- Have digits and punctuation characters as well as letters.

[19] California County Information Services Directors Association, *California Counties "Best Policies" for the Countywide Information Security Program*, 2003.

- Include at least eight alphanumeric characters.
- Not be a single word in any language, slang, dialect, or jargon.
- Not be based on personal information such as the name of the user or user's family members.
- Never be written (unless stored in a locked safe for recovery purposes) or stored online.

Recommendation

25. SFMTA should develop, implement, and communicate a password standard in Trapeze that incorporates industry best practices such as complexity standards (e.g., minimum length of eight characters, mix of alphabetical and numeric characters) and a policy that passwords will expire after a reasonable duration.

APPENDIX: DEPARTMENT RESPONSE

SFMTA
Municipal Transportation Agency

January 8, 2013

Ms. Tonia Lediju
Director of City Audits
Office of the Controller
1 Dr. Carlton B. Goodlett Place, Room 316
San Francisco, CA 94102

Re: SFMTA Lacks Effective Controls Over Its Payroll Process and Timekeeping System for Transit Operators

Dear Ms. Lediju,

I would like to thank you and your staff for the review of the SFMTA timekeeping and payroll protocols and procedures. We concur with a number of your findings and recommendations and agree that we can improve procedures and protocols surrounding operator payroll.

Recommendations such as tracking service for special events have already been implemented and are noted in the response matrix. While we agree that cross-training additional staff is beneficial and additional cross-training will be implemented, SFMTA employees across three departments ensure that operator payroll and data integrity is processed in an accurate and timely manner. We plan to have many of the remaining recommendations with which SFMTA concurs in place by the end of fiscal year 2013.

Thank you for your efforts. There is always room for improvement and we welcome the recommendations that will assist in improving our payroll and timekeeping systems.

Sincerely,

Edward D. Reiskin
Director of Transportation

One South Van Ness Ave.
Seventh Floor
San Francisco, CA 94103
Tele: 415.701.4500
www.sfmta.com

For each recommendation, the responsible agency should indicate whether it concurs, does not concur, or partially concurs. If it concurs with the recommendation, it should indicate the expected implementation date and implementation plan. If the responsible agency does not concur or partially concurs, please provide an explanation and an alternate plan of action to address the identified issue.

AUDIT RECOMMENDATIONS AND RESPONSES

Recommendation	Response
The San Francisco Municipal Transportation Agency (SFMTA) should:	
1. Develop and implement procedures in which supervisors verify for accuracy and approve unscheduled overtime.	Concur. Implementation Date: February 2013
2. Review and assess the feasibility of adopting new technologies such as new communications systems, computer-aided dispatch, and automated vehicle location packages to allow SFMTA to better manage overtime, with the aim of reducing unscheduled overtime.	Concur. SFMTA is replacing and upgrading the current radio system from the 1970s with a modern computer aided-dispatch communications system. The system will integrate dispatching and vehicle tracking functions. Implementation: Vendor under contract and completion date is expected in 2015.
3. Develop and implement procedures in which the employee who verifies and approves unscheduled overtime does not also enter these hours in Trapeze.	Concur. Implementation Date: February 2013
4. Enforce its procedures to require that all unscheduled overtime is documented on an overtime slip.	Concur. Implementation Date: January 2013

Recommendation	Response
5. Ensure that all overtime slips are retained in accordance with SFMTA's record retention policy.	Concur. Implementation Date: January 2013
6. Add specific overtime slip completion requirements for transit operators in the dispatch standard operating procedure.	Concur. Implementation Date: February 2013
7. Establish a procedure to ensure that all unscheduled overtime slips are adequately completed and submitted. The procedure should include that dispatchers will reject and return to transit operators insufficiently or incorrectly completed slips. The procedure should also include a periodic internal audit process of checking slips for existence and accuracy.	Concur. Implementation Date: March 2013
8. Periodically train all dispatchers to follow standard time-entry procedures and, as part of exception-based time-entry, to spot specific anomalies in transit operators' reported hours.	Concur. Implementation Date: June 2013
9. Establish and document a formal process to ensure that any change to the Trapeze system related to the transit operators' memorandum of understanding be: • Clearly documented at the time of the change. • Independently reviewed, approved, and tested before it is implemented.	Concur. Implementation Date: June 2013

Recommendation	Response
10. Develop and implement procedures to consistently reconcile data in the Trapeze system to data in PPSD's payroll system after each pay period. A supervisor should review and approve the reconciliations.	Concur. Implementation Date: March 2013
11. Immediately change (to ineligible) the status in the Trapeze system of all transit operators identified as eligible to receive expert operator premium pay that are not on the list of those qualified for this pay.	Concur. Implementation Date: Completed and procedure in place by January 2013
12. Establish procedures to periodically review Trapeze system-generated reports on employees' pay status and pay status changes to ensure that all premium pays, including expert operator premium pay, are appropriately applied.	Concur. Expert operator premium pay already fixed. Implementation Date: February 2013
13. Ensure that Trapeze system controls prevent transit operators from receiving birthday pay more than once per year.	Concur. Implementation Date: Completed
14. Continue to establish index codes to identify the costs associated with specific scheduled and generic unscheduled special events. In doing so, SFMTA should identify specific recurring and one-time scheduled events whose sponsors SFMTA may be able to bill to reimburse it for the extra costs it incurs, including transit operator overtime, to provide transit service.	Concur. Implementation Date: Completed

Recommendation	Response
15. Periodically reassess the need for each pay code in Trapeze and deactivate obsolete pay codes.	Concur Implementation Date: March 2013
16. Develop a single, comprehensive, up-to-date policies and procedures manual for its payroll process that is in accordance with citywide payroll procedures.	Concur. Implementation Date: Once the City provides comprehensive payroll procedures, we will incorporate those procedures with internal SFMTA specific practices and procedures.
17. Establish and segregate the roles and responsibilities of personnel supporting Trapeze. These roles must clearly reflect SFMTA's overall business needs and information technology objectives and ensure sufficient back-up support and cross-training to reduce the risk of major disruption to Trapeze system operations.	Concur. Implementation date: September 2013
18. Review and formally determine which transactions and system changes in Trapeze and its related Oracle database are most critical. Apply the audit trail functionality to the most critical transactions and changes if this can be done without significantly degrading system performance.	Partially concur. We agree that an audit trail is essential and will work to implement unless it degrades system performance and prevents timely, efficient timekeeping and payroll functions for our 2,000+ operators. Implementation date: Assess feasibility by June 2013.
19. Develop policies and procedures to review, analyze, and retain audit trail logs.	Concur. Implementation date: March 2013

Recommendation	Response
20. Ensure that all system changes in Trapeze and its related Oracle database are tested and approved by appropriate SFMTA personnel.	Concur. This is currently performed informally. We will formalize documentation procedures. Implementation date: June 2013
21. Update its information technology change management policies and procedures, at minimum annually, to reflect current practices and to meet SFMTA's business objectives. Additionally, the policies and procedures should be approved and communicated to all staff.	Concur. Implementation date: June 2013
22. Review the current security profiles for all Trapeze users and administrators and ensure that the system access rights of employees who no longer need this access are immediately terminated.	Concur. Implementation date: February 2013
23. Establish written procedures and a schedule for periodically reviewing user lists and the associated access rights for Trapeze.	Concur. Implementation date: June 2013
24. Review and assess generic Trapeze accounts to determine if they are necessary and, if so, whether users' access levels are adequately limited. Disable unnecessary generic accounts and reduce unnecessary access levels.	Partially concur. Current generic accounts have read-only access and cannot make changes to Trapeze. We will assess whether these are needed and make modifications if necessary. Implementation date: March 2013

Recommendation	Response
25. Develop, implement, and communicate a password standard in Trapeze that incorporates industry best practices such as complexity standards (e.g., minimum length of eight characters, mix of alphabetical and numeric characters) and a policy that passwords will expire after a reasonable duration.	Concur. Implementation date: March 2013