



**CITY OF DALLAS**

**Dallas City Council**

**Mayor**

Tom Leppert

**Mayor Pro Tem**

Dwaine R. Caraway

**Deputy Mayor Pro Tem**

Pauline Medrano

**Council Members**

Jerry R. Allen

Tennell Atkins

Carolyn R. Davis

Vonciel Jones Hill

Angela Hunt

Delia Jasso

Sheffield Kadane

Linda Koop

Ann Margolin

Ron Natinsky

David A. Neumann

Steve Salazar

**Office of the City Auditor**

**Audit Report**

**AUDIT OF  
SELECTED GENERAL COMPUTER CONTROLS  
OVER VARIOUS REVENUE SOURCES  
FOR THE DEPARTMENT OF  
PARK AND RECREATION**

(Report No. A11-002)

**October 8, 2010**

**City Auditor**

Craig D. Kinton

## Table of Contents

	Page
<b>Executive Summary</b>	1
<b>Audit Results</b>	
Section I: General Computer Controls Are Not Implemented	5
Section II: Change Management	9
Section III: Computer Operations	11
<b>Appendices</b>	
Appendix I – Background, Objective, Scope and Methodology	13
Appendix II – Major Contributors to This Report	17
Appendix III – Management’s Response	18

## Executive Summary

Selected general computer controls for the Class and Club Prophet Point of Sale (POS) applications, which support revenue transaction processing for approximately 72 percent of the \$11.8 million Department of Park and Recreation (PKR) Fiscal Year (FY) 2010 budgeted revenue, are generally not well designed or properly implemented.

Specifically, the PKR information technology function, which operates independently of the City's Department of Communication and Information Services (CIS), has not established general computer controls over change management, security administration, and computer operations for these POS applications. Without general computer controls over the Class and Club Prophet POS applications, PKR cannot ensure the accuracy and completeness of revenue processing.

At the request of the Office of the City Auditor, the PKR information technology function completed a general computer control self-assessment using Control Objectives for Information and related Technology (CoBIT) criteria. This self-assessment is an important evaluation tool to help PKR identify risks and correct control deficiencies to minimize those risks.

### General Computer Controls

General computer control applies to all information systems—mainframe, minicomputer, network, and end-user environments.

General computer controls includes entity wide security program planning [security], management, control over data center operations [computer operations], system software acquisition and maintenance [change management], access security [security] ...More specifically:

- **System software (change management)** control includes control over the acquisition, implementation, and maintenance of all system software, including operating system, data-based management systems, telecommunications, security software, and utility programs.
- **Access security (security)** control protects the systems and network from inappropriate access and unauthorized use by hackers and other trespassers or inappropriate use by...personnel. Specific control activities include...restrictions on users to allow access only to system functions that they need; software and hardware "firewalls" to restrict access to assets, computers, and networks by external persons; and frequent changes of passwords and deactivation of former employees' passwords.
- **Data center and client-server operations (computer operations)** controls include backup and recovery procedures, and contingency and disaster planning. In addition, data center operations controls also included job set-up and scheduling procedures and controls over operator activities.

**Source:** General Accounting Office, Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1), pages 16-17

The PKR self-assessment identified general computer controls deficiencies discussed in Sections II, III and IV of this report. PKR management determined that:

- 39 percent of the Club Prophet and 22 percent of the Class POS applications' general computer controls are at a Control Maturity Stage 1
- 35 percent of the Club Prophet and 39 percent of the Class POS applications' general computer controls are at a Control Maturity Stage 2

**Six Maturity Stages of CoBIT  
Maturity Model for Internal Control**

The CoBIT Maturity Model enables benchmarking and identification of necessary capability improvements based on evaluating how current processes meet business and information technology goals. Maturity modeling for management and control over information technology processes is based on a method of evaluating the organization so it can be rated on a maturity level from:

Stage 0 – Nonexistent  
Stage 1 – Initial/Ad Hoc  
Stage 2 – Repeatable, but Intuitive  
Stage 3 – Defined Process  
Stage 4 – Managed and Measureable  
Stage 5 – Optimized

**Source:** Control Objectives for Information and related Technology (CoBIT) 4.1, pages 17-19

According to the CoBIT *Maturity Model for Internal Control*, general computer controls between Control Maturity Stage 1 and Control Maturity Stage 2 indicate that:

- There is some recognition of the need for internal controls; therefore, the approach to risk and control requirements is *ad hoc* and disorganized
- The existing internal controls are *repeatable, but intuitive*; therefore, they are inconsistently performed

The PKR recently implemented the Club Prophet and Class POS applications as revenues increased in the Athletic Field and Rental Reservations, Community Recreation Centers, and the full-service golf facilities.

Therefore, it is reasonable to expect that PKR's primary objective would be to establish the business processes supported by each of these POS applications rather than focusing on the establishment of the general computer controls.

The Class POS application supports approximately \$4.1 million in annual revenue transaction processing for Athletic Field and Rental Reservations and the Community Recreation Centers. The Club Prophet POS application supports approximately \$4.3 million in annual revenue transaction processing for the full-service golf facilities, including the golf range and the golf pro shops.

The report issues and associated recommendations related to certain aspects of security administration have been omitted from this report. Our decision to exclude this information is based on:

**An Audit Report on –  
Selected General Computer Controls Over Various Revenue Sources  
For the Department of Park and Recreation**

---

- Government Auditing Standards, July 2007 Revision, Sections 8.38 – 8.42 Reporting Confidential or Sensitive Information; and,
- Texas Government Code Section 552.139. EXCEPTION: GOVERNMENT INFORMATION RELATED TO SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS

Security Administration general computer control issues have been communicated to the appropriate PKR personnel in the *Confidential Security Administration Limited Use Report – Audit of Selected General Computer Controls Over Various Revenue Sources for the Department of Park and Recreation*.

The audit objective was to evaluate selected PKR general computer controls over POS applications which support processing of approximately 72 percent of the PKR revenues for FY 2010. The scope of the audit covered the general computer control areas of change management, security administration, and computer operations from October 2009 to July 2010.

Management's response to this report is included as Appendix III.

# Audit Results

## Overall Conclusion

Selected general computer controls for the Class and Club Prophet Point of Sale (POS) applications, which support revenue transaction processing for approximately 72 percent of the \$11.8 million Department of Park and Recreation (PKR) Fiscal Year (FY) 2010 budgeted revenue, are generally not well designed or properly implemented.

Specifically, the PKR information technology function, which operates independently of the City's Department of Communication and Information Services (CIS), has not established general computer controls over change management, security administration, and computer operations for these POS applications. Without general computer controls over the Class and Club Prophet POS applications, PKR cannot ensure the accuracy and completeness of revenue processing.

## Section I: General Computer Controls Are Not Implemented

### Policies and Procedures Were Not Established or Documented

#### CoBIT Recommends

The CoBIT process has generic control requirements that should be considered together with process control objectives. These include the following:

- Policy, Plans, and Procedures: Define and communicate how all policies, plans, and procedures that drive an information technology process are documented, reviewed, maintained, approved, stored, communicated, and used for training.
- Process Ownership: Assign an owner for each information technology process
- Process Repeatability: Design and establish each key information technology process such that it is repeatable and consistently produces the expected results
- Roles and Responsibilities: Define the key activities and end deliverables of the process

Effective controls reduce risk, increase the likelihood of value delivery, and improve efficiency because there will be fewer errors and more consistent management approach.

**Source:** Control Objectives for Information and related Technology (CoBIT) v 4.1, pages 14-15

Policies and procedures to support the control activities related to change management, security administration, and computer operations were generally not established or documented for the Class and Club Prophet POS applications. In addition, a process to consider the development and management of the policies and procedures is not in place. As a result, certain information technology control activities are not performed consistently or performed at all.

For example, server configuration backups are not performed on a pre-determined schedule. The Club Prophet POS server configuration backup is not performed regularly or as frequently as the Class server configuration backup

which is performed at least quarterly. As a result, the Club Prophet POS server may not be available for timely recovery when the server malfunctions and golf tee-times may not be scheduled through the POS application.

Additionally, neither of these POS applications has enabled password policies to ensure that inappropriate users do not have access to add, delete, or modify revenue transactions. Therefore, there is increased risk that the generated revenue transactions might not accurately reflect actual transactions.

Without up-to-date policies and procedures, information technology control activities may not be consistently performed or performed at all. For example, both the POS applications rely on the vendor for change management; however, there is no clear policy on how to manage these vendor services. So, there is no identification of potential risks such as vendor access to data and no accountability for services received.

Current policies and procedures that would formalize the information technology activities would help the information technology function execute job responsibilities consistently, properly assign accountability, and effectively manage information technology processes.

## **Recommendation I**

We recommend the Director of PKR ensure that for POS applications:

- Policies and procedures for change management, security administration, and computer operations are established and documented
- Policies and procedures consider unique circumstances, such as reliance on third party services

Please see Appendix III for management's response to the recommendation.

## Certain General Computer Controls Support Provided by Vendors Are Not Appropriately Documented and Managed

The PKR uses third party service providers (vendors) to provide certain general computer controls support for the Class and Club Prophet POS applications, such as change management, without a formal operating level agreement (OLA). Although software license agreements are in place, these agreements do not sufficiently cover the expanded support currently provided by the vendors. Without adequate OLAs between PKR and the vendors, there is not a clear definition of roles, responsibilities, and expectations. Additionally, the PKR may become too vendor-dependent which could result in unforeseen costs and complexities in managing the applications.

### Best Practice

A goal of third party relationships is to ensure transparency and understanding of information technology costs, benefits, and strategy, policies, and services levels.

An internal control activity that can be implemented to meet this goal includes monitoring and measuring performance.

**Source:** Control Objectives for Information and related Technology (CoBIT) v 4.1, page 107.

For example, PKR does not have a process in place to track, evaluate, and manage application customizations made by the vendor. At PKR's request, the Club Prophet POS application was customized significantly by the vendor to adjust the application for the City's unique business structure for golf operations. Although the vendor complied with these customization requests, the vendor does not have the responsibility for:

- Evaluating the impact of the customizations on future Club Prophet POS application upgrades or the future maintenance of these customizations
- Providing the information necessary to document application requirements, if the City decides to use a different vendor in the future

In addition, PKR contracts with vendors that establish and manage golf pro-shops do not consider information security requirements, such as sharing of passwords or installing anti-virus software on the work stations (e.g., desktops, laptops). Therefore, there is a risk that a non-City employee at the golf pro shop could inadvertently or maliciously commit fraud that affects the City's revenue or introduce a virus to the server.

Managing vendors appropriately is accomplished by defining roles, responsibilities, and expectations through OLAs and then monitoring vendor activities for compliance with those agreements.

## **Recommendation II**

We recommend the Director of PKR:

- Establish and document OLAs with vendors to ensure that roles, responsibilities, and expectations are defined
- Monitor vendor agreements periodically to verify compliance with OLAs

Please see Appendix III for management's response to the recommendation.

## Section II: Change Management

### Application Changes Are Not Formally Approved, Planned, and Tested

Changes to the data and the system for the Class and Club Prophet POS applications are not always formally approved, planned, and tested prior to implementation. Instead, changes to the data and the system are completed in an ad-hoc manner. Additionally, PKR does not periodically review changes that were implemented to validate that only planned and authorized changes were introduced into production. Ad-hoc change management could jeopardize the reliability of data because errors or incomplete changes may be introduced into production and disrupt business operations. Specifically, PKR does not have formal processes in place to:

#### Track user requests and approvals for change requests

- Class POS – The vendor’s online customer inquiry portal, which PKR relies on to manage all change requests, does not capture sufficient detail regarding the change requests
- Club Prophet POS – There is not a consistent method to track changes and communicate the impact of these changes to all vendors and the application users because change requests are initiated through various methods (e.g., phone call, e-mail) and from various sources (e.g., PKR personnel or golf pro shop vendors)

#### Test change requests

- Class POS – Testing is completed only for upgrades and often with limited user involvement. If testing is performed, the supporting documentation is not retained for future reference.
- Club Prophet POS – Testing of change requests is often completed by the vendor and often with limited PKR user involvement

Migration of change requests to production

- Club Prophet POS – Duties are not properly segregated because PKR has granted full production access to the vendor to allow the vendor to implement changes (e.g., the vendor develops the change request and migrates the change request into production)

**Segregation of Duties**

A basic internal control that prevents or detects errors and irregularities by assigning responsibility to separate individuals for initiating and recording transactions and custody of assets to separate individuals. Commonly used in large information technology organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

**Source:** Control Objectives for Information and related Technology (CoBIT) 4.1, Appendix VII, page 193.

The PKR has not implemented compensating controls, such as: (1) limiting vendor access to an as-needed basis; (2) monitoring the vendor's access through a combination of reports and audit logs; and, (3) evaluating whether the vendor's access and the change request log appear to be in sync.

Change management procedures that include formal processes for tracking change requests, performing an appropriate level of testing with user

involvement, and segregating duties helps to ensure that only those changes to data and systems which are critical to business operations are introduced into production.

**Recommendation III**

We recommend the Director of PKR develop, document, and implement formal change management procedures that are standard, reliable, and consistent so that only approved, planned, and tested changes are made to data and systems for the POS applications.

Please see Appendix III for management's response to the recommendation.

## Section III: Computer Operations

### Data Backup and Restoration Processes Are Not Adequate

The PKR does not have adequate processes for backup and restoration of revenue data (e.g., hardware and software systems and data sources) for non-disaster recovery purposes. As a result, data might not be available during non-disaster situations, such as a virus attack, and could impair PKR's ability to serve the citizens. The objective of non-disaster data backup and recovery is so PKR can continue to conduct business without interruptions.

#### Scheduling and Monitoring of Backups

The PKR schedules daily backups for both POS applications data; however, PKR does not retain documentation to show that the backups were completed as scheduled and backup processing was resolved.

#### Off-site Tape Rotation

The PKR data is backed up to an external drive; however, the external drive is connected to the primary server and not removed off-site to an alternate location. As a result, the data backups are subjected to the same concerns as production data located on-site. Therefore, during business interruptions, data is not available for recovery.

#### Data Restoration

Backup data is not tested periodically to ensure that backups can be recovered and are available outside of the normal disaster recovery testing. The PKR information technology personnel stated the Class POS application data is often restored to a training database, but the process is not formalized. Conversely, the Club Prophet POS application data is not restored at all.

#### Definitions

**Backup:** Copy of operational data, application, file, or system that can be used to restore the data, application, file, or system.

**Restore:** To recover data, application, file, or system to a previous state not under a disaster recovery environment.

**Source:** Administrative Directive 2-34, *Data Backup and Recovery, Standard, and Procedures for the Mainframe and Servers* Page 2, Section 4 Definitions

## **Recommendation IV**

We recommend the Director of PKR establish data backup and restoration procedures to ensure that data is available during non-disaster recovery purposes.

Please see Appendix III for management's response to the recommendation.

## Appendix I

### Background, Objective, Scope and Methodology

#### Background

The Department of Park and Recreation (PKR) generates revenues from several divisions; however, there are three divisions which contribute to approximately 72 percent of the total PKR budgeted revenues for Fiscal Year (FY) 2010. The three divisions are the Athletic Field and Rental Reservations (Reservations), Community Recreation Centers, and Golf Facilities. The Reservations and Community Recreation Centers work in tandem since the revenue that is generated uses the same resources, but for different purposes (e.g., field reservation for youth games versus concession sales at youth game events).

All three divisions and their revenue processing are managed by two point-of-sale (POS) applications, Class and Club Prophet. These POS applications are supported by the PKR information technology group, which operates independently of the Department of Communication and Information Services (CIS).

#### Athletic and Field Reservations

The Reservations division supports all athletic and field reservations and manages all transactions related to facility rentals, special events and runs. The 47 Community Recreation Centers are autonomously managed and handle a myriad of transactions not supported by the Reservations division. Some of the transactions that the Community Recreation Centers support are the issuance of identification cards, contract fee lessons, staff taught lessons, recreation center room reservations, and limited field reservations that are not handled by the Reservations division.

The Reservations and the Community Recreation Center divisions' revenues are collected in cash, check, or credit card. The budgeted estimated revenues for the Reservations and the Community Recreation Centers divisions are approximately \$4.1 million for FY 2010. All Reservations and Community Recreation Centers divisions' revenue processing is managed through the Class POS application. The Class POS system uses a Microsoft SQL database and operates on a Windows 2000 platform.

## **Golf Facilities**

The City of Dallas owns six full-service golf facilities. A full-service facility means that the facility has an independently owned and managed golf pro shop, has the golf range, offers golf lessons taught by certified professionals, and can host organized golf tournaments. The golf pro shop operation is owned by independent business owners who contract with the City for the use of the golf course. The City owns and maintains the golf course and the business owner is responsible for all management of the golf pro shop including the purchasing and selling of food and drinks, clothing, and other golf related merchandise (e.g., golf balls).

The budgeted estimated revenues for golf are approximately \$4.3 million for FY 2010. Golf revenues are collected in cash, check, or credit card. The City uses the Club Prophet POS application to support the processing of transactions at each golf facility. The Club Prophet POS system uses a Microsoft SQL database and operates on a Windows 2000 platform.

## **Objective, Scope and Methodology**

We conducted this audit under the authority of the City Charter, Chapter IX, Section 3, and in accordance with the Fiscal Year 2010 Audit Plan approved by the City Council. This performance audit was conducted 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The audit objective was to evaluate selected PKR general computer controls over POS applications which support processing of approximately 72 percent of the PKR revenues. The scope of the audit covered the general computer control areas of change management, security administration, and computer operations from October 2009 to July 2010.

The report issues and associated recommendations related to security administration have been omitted from this report. Our decision to exclude this information is based on:

- Government Auditing Standards, July 2007 Revision, Sections 8.38 – 8.42 Reporting Confidential or Sensitive Information; and,

- Texas Government Code Section 552.139. EXCEPTION:  
GOVERNMENT INFORMATION RELATED TO SECURITY OR  
INFRASTRUCTURE ISSUES FOR COMPUTERS

Security administration general computer controls issues have been communicated to the appropriate PKR personnel in the *Confidential Security Administration Limited Use Report - Audit of Selected General Computer Controls Over Various Revenue Sources for the Department of Park and Recreation*.

To achieve the audit objective, we performed the following procedures:

- Reviewed existing policies and procedures and the City's Administrative Directives (ADs) related to information technology and compared them to the best practices identified in Control Objectives for Information and related Technology (CoBIT)
- Benchmarked the general computer controls by using the Office of the City Auditor's current and prior audit knowledge, prior results from external auditors, and the CoBIT *Maturity Model for Internal Control*
- Evaluated general computer controls for compliance with the best practices
- Interviewed personnel who support the PKR information technology infrastructure (mainframe, network, and client server environments), as well as the personnel involved in the revenue transaction processing
- Reviewed various documents, including PKR's FY 2010 budget, selected daily cash reports, contracts, organization charts, etc.

Additionally, we completed a reasonableness analysis to determine which industry best practice framework would be most relevant to the City's environment. We verified that the CoBIT framework initially served as the framework for the contents in the ADs as identified in AD 2-02, *Systems Development Life Cycle*. Additionally, the Texas Local Government Code that was cited in the ADs and the Federal Information System Controls Audit Manual (FISCAM) developed by the Government Accountability Office (GAO) were considered. We also verified that the City's external auditors use the CoBIT framework in the annual financial audits. As a result, the Office of the City Auditor considered the CoBIT framework a reasonable best practice framework against which to evaluate general computer controls.

**An Audit Report on –  
Selected General Computer Controls Over Various Revenue Sources  
For the Department of Park and Recreation**

---

Control matrices for security administration, change management, and computer operations were generated and shared with the Department of Park and Recreation (PKR) management during the course of fieldwork.

## Appendix II

### Major Contributors to This Report

Carol A. Smith, CPA, CIA, CFE – Assistant City Auditor  
Mamatha Sparks, CIA, CISA – Project Manager  
Theresa Hampden, CPA – Quality Control Manager

## Management's Response

Memorandum

**RECEIVED**  
SEP 24 2010  
City Auditor's Office



DATE: September 23, 2010

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report:  
Audit of Selected General Computer Controls Over Various Revenue Sources for the  
Department of Park and Recreation

Our responses to the audit report recommendations are as follows:

**Recommendation I:**

We recommend the Director of PKR ensure that for POS applications:

- Policies and procedures for change management, security administration, and computer operations are established and documented
- Policies and procedures consider unique circumstances, such as reliance on third party services

**Management Response / Corrective Action Plan**

Agree  Disagree

The Park and Recreation Department is establishing policies and procedures for change management, security administration and computer/server operations that are commonly used as a means of standardizing future audit processes.

**Implementation Date**

March 2011

**Responsible Manager**

Ken Brack

**An Audit Report on –  
Selected General Computer Controls Over Various Revenue Sources  
For the Department of Park and Recreation**

---

**Recommendation II:**

We recommend the Director of PKR:

- Establish and document OLAs with vendors to ensure that roles, responsibilities, and expectations are defined
- Monitor vendor agreements periodically to verify compliance with OLAs

**Management Response / Corrective Action Plan**

Agree  Disagree

PKR will establish an OLA with Club Prophet to cover the Golf Point of Sale system. PKR will seek modification of the current license/maintenance agreement with Active Network to incorporate language that is consistent with an operating level agreement.

**Implementation Date**

January 2011

**Responsible Manager**

Ken Brack

**Recommendation III:**

We recommend the Director of PKR develop, document, and implement formal change management procedures that are standard, reliable, and consistent so that only approved, planned, and tested changes are made to data and systems for the POS applications.

**Management Response / Corrective Action Plan**

Agree  Disagree

The Park and Recreation Department will implement change management procedures for both Active Network and Club Prophet systems. These procedures will be based on best practices identified in CoBIT's General computer Controls CC-1 through 8. A record of updates and changes made to the systems will be documented and maintained in a database to provide historical record.

**Implementation Date**

March 2011

**Responsible Manager**

Ken Brack

"Dallas: The City That Works: Diverse, Vibrant, and Progressive."

**An Audit Report on –  
Selected General Computer Controls Over Various Revenue Sources  
For the Department of Park and Recreation**

---

**Recommendation IV:**

We recommend the Director of PKR establish data backup and restoration procedures to ensure that data is available during non-disaster recovery purposes.

**Management Response / Corrective Action Plan**

Agree  Disagree

The Park and Recreation Department will develop data backup and restoration procedures and will deploy those procedures to server support staff in order to validate backups and run test restores on a routine basis. The department will also develop procedures for off-site backup storage.

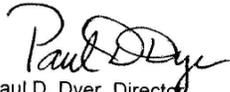
**Implementation Date**

November 2010

**Responsible Manager**

Ken Brack

Sincerely,



Paul D. Dyer, Director  
Dallas Park and Recreation Department

C: Barbara Kindig  
Ken Brack