



CITY OF DALLAS

Dallas City Council

Mayor

Tom Leppert

Mayor Pro Tem

Dwayne 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
FOR THE DALLAS POLICE DEPARTMENT AND
THE DALLAS FIRE-RESCUE
PRIMARILY ADMINISTERED BY THE
DEPARTMENT OF COMMUNICATION AND
INFORMATION SERVICES**

(Report No. A10-014)

June 25, 2010

City Auditor

Craig D. Kinton

Table of Contents

	Page
Executive Summary	1
Audit Results	
Section I: General Computer Controls Deficiencies Continue	6
Section II: Change Management	12
Section III: Computer Operations	14
Appendices	
Appendix I – Background, Objective, Scope and Methodology	16
Appendix II – Major Contributors to This Report	20
Appendix III – Management’s Response	21

Executive Summary

Change management, security administration, and computer operations general computer controls for the Dallas Police Department (DPD) and the Dallas Fire-Rescue (DFR) are generally not well designed or operating effectively. As a result, significant general computer controls are not in place to prevent, detect, and monitor critical functionality, such as unauthorized access to confidential data and files.

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:

- 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 Department of Communication and Information Services (CIS) personnel in the *Limited Use Report – DPD/DFR Security Administration*.

The CIS, which has primary administrative responsibility for DPD's and DFR's general computer controls, has not developed a framework that describes the City's general computer controls. As a result, CIS does not have a formal documented methodology that links the City's business requirements to daily functions, organizes information technology activities into processes, and provides the information necessary to conduct control self-assessments. Without control self-assessments, CIS cannot easily identify risks and correct general computer control deficiencies to minimize those risks. In addition, City management, the Office of the City Auditor, and external auditors do not have a

Internal Control

The policies, plans, and procedures and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

General Computer Controls

Controls, other than application controls, which relate to the environment within computer-based application systems.

The objectives of general computer controls are to ensure the proper development and implementation of applications, the integrity of the program and data files, and of computer operations.

Source: Control Objectives for Information and related Technology (CoBIT) 4.1, Appendix VII – Glossary, pages 190 and 191

consistent approach to evaluate whether general computer controls are improving.

In the absence of a CIS general computer control self-assessment and after identifying the significant general computer controls deficiencies discussed in Sections II and III of this report and in the *Limited Use Report – DPD/DFR Security Administration* provided to CIS, it was determined that the general computer controls are at a Control Maturity Stage 2. According to the Control Objectives for Information and related Technology (CoBIT) *Maturity Model for Internal Control*, a Control Maturity Stage 2 indicates that controls are “Repeatable, but Intuitive”. In other words:

- General computer controls are in place, but are not documented and, therefore, operation is dependent on the knowledge and motivation of individuals
- Many general computer control deficiencies exist and are not adequately addressed and the impact may be severe
- Management’s actions to resolve general computer control issues are not prioritized and, therefore, assessment of general computer controls occurs only when needed for selected Information Technology processes

In addition, the data necessary for critical DPD and DFR functions may not be available. For example:

- The Police Reports application was shut down by the application vendor in August 2009 because the application vendor had unauthorized and unmonitored access to the application’s source code. The shut down caused DPD and others (e.g., citizens) to lose access to automated information related to on-going crime activities within the City.
- The Computer Aided Dispatch (CAD) application, which is a 24/7 application used by both DPD and DFR, was not functioning as designed because a virus attack made the application inoperable. According to CIS, the 911 system was not affected; however, the virus attack disabled the CAD application for 13 hours on May 13, 2009. As a result, DPD and DFR had to resort to slower manual processes. Therefore, during this time period, DPD and DFR may not have been positioned to respond as promptly to emergency requests from citizens.

For several years, the Office of the City Auditor and the external auditors have reported the same or comparable general computer control deficiencies. Based upon the results of this audit, CIS has either not addressed or has not fully

**An Audit Report on –
Selected General Computer Controls for the Dallas Police Department and Dallas Fire-Rescue
Primarily Administered by the Department of Communication and Information Services**

addressed these general computer control deficiencies which could have serious consequences for the City.

The audit objective was to evaluate selected general computer controls for DPD and DFR which provide critical public safety services to the citizens; however, DPD and DFR general computer controls are primarily administered by CIS. As a result, the issues discussed in this report are primarily addressed to CIS. The scope of the audit covered the general computer control areas of change management, security administration, and computer operations from February 2009 through July 2009.

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

Audit Results

Overall Conclusion

Change management, security administration, and computer operations general computer controls for the Dallas Police Department (DPD) and the Dallas Fire-Rescue (DFR) are generally not well designed or operating effectively. As a result, significant general computer controls are not in place to prevent, detect, and monitor critical functionality, such as unauthorized access to confidential data and files.

The Department of Communication and Information Services (CIS) has primary administrative responsibility for DPD's and DFR's general computer controls. As a result, the issues discussed in this report are primarily addressed to CIS.

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 control issues have been communicated to the appropriate CIS personnel in the *Limited Use Report – DPD/DFR Security Administration*.

Section I: General Computer Controls Deficiencies Continue

A General Computer Controls Framework Has Not Been Developed

The CIS has not developed a framework that describes the City's general computer controls. As a result, CIS does not have a formal documented methodology that links the City's business requirements to daily functions, organizes information technology activities into processes, and provides the information necessary to conduct control self-assessments. Without control self-assessments, CIS cannot easily identify risks and correct control deficiencies to minimize those risks. In addition, City management, the Office of the City Auditor, and external auditors do not have a consistent approach to evaluate whether general computer controls are improving.

The CIS was given an opportunity to provide a self-assessment of the City's general computer controls and their associated control maturity stage using the Control Objectives for Information and related Technology (CoBIT) *Maturity Model for Internal Control* (CoBIT MM) (see textbox). The purpose of performing the self-assessment was to:

- Establish a control maturity stage to formalize how well the City's current information technology processes are managed
- Set an initial point for CIS, the Office of the City Auditor, and external auditors to measure CIS's progress in improving general computer controls

Over time, as CIS improves the general computer controls framework, the control maturity stage assessment would also improve. Thus, each increase in maturity stage should reduce the City's risk that general computer controls are not well designed or operating effectively. As a result, the City's information technology processes would become more predictable, efficient, and cost effective.

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 Measurable
- Stage 5 – Optimized

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

The CIS management declined the self-assessment opportunity, stating that CIS did not use CoBIT or the CoBIT MM. (Note: CoBIT is an established guideline for information technology control design, maintenance, and monitoring and is used by both computing professionals, the Office of the City Auditor, and external auditors). The CIS, however, did not provide alternative guidelines or a general computer controls self-assessment.

According to the CoBIT 4.1 framework, for an entity to be successful in delivering against business requirements, management should establish a general computer controls framework and perform general computer control self-assessments to measure progress.

Recommendation I

We recommend that the Director of CIS establish a general computer controls framework that aligns with best practices that are commonly used and accepted in the United States – such as CoBIT, and one that provides City Council, management, as well as the Office of the City Auditor and external auditors, a consistent means to evaluate whether general computer controls are improving.

We also recommend that the Director of CIS perform regular general computer control self-assessments to ensure that the general computer controls framework is designed and operating as intended.

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

Policies and Procedures Were Generally Not Available and Do Not Consistently Align With Information Technology Administrative Directives

Change management, security administration, and computer operations policies and procedures were generally not current or not available. If policies and procedures were available, they were either outdated or did not consistently align with the City’s Administrative Directives (AD) related to information technology. (See Table I below).

Table I

Summary of Information Technology Related Administrative Directives and CIS Policies Provided

General Computer Controls Area	Administrative Directive (AD)	Last Updated	Policy (ies) Provided (Y/N)	Aligned with AD (Y/N)
Change Management	2-28, <i>Change Management of Information Technology</i>	5/27/2004	Y	N
Security Administration	2-24, <i>Computer Security</i>	7/15/1998	N	N/A
Security Administration	2-33, <i>Acceptable use of City Provided e-mail and Internet Services</i>	7/31/2001	N	N/A
Computer Operations	2-25, <i>Data Classification and Ownership</i>	7/15/1998	N	N/A
Computer Operations	2-34, <i>Data Backup and Recovery Policy, Standard and Procedures for the Mainframe and Servers</i>	5/27/2004	Y	N

Source: Information technology related ADs and CIS policies provided

Furthermore, these ADs have not been updated to incorporate the City’s information technology changes over the past five to ten years. The AD 2-24, *Computer Security*, focuses predominantly on securing a mainframe environment with limited consideration of the risks related to the City’s growing client server environment. For example, the two DPD mainframe applications, the Direct Entry Field Reporting System (DEFRS) and the Direct Entry Arrest Reporting System (DEARS) are in the process of being replaced by client-server architecture.

Definitions

Mainframe: Largest data processing system employed in controlling very complex industrial processes, crunching extremely large numbers at extremely high speeds, storing massive amounts of data, generating life-like animation, processing millions of real-time transactions, and serving thousands of simultaneous users.

Client-Server: Technology that separates computers and application software into two categories – clients and servers – to better employ available computing resources and share data processing loads.

Source: *www.businessdictionary.com*

In addition, without up-to-date policies and procedures and ADs, DPD and DFR information technology personnel who are currently managing their own information technology functions or supporting CIS during the transition to a centralized information technology function do not know CIS standards or requirements. As a result, several basic general computer controls continue to be by-passed which can impact the availability, reliability, and confidentiality of the systems and the data. For example, changes to data and systems are not formally approved, planned, tested, and recoverable. (Refer to page 12 of this report for further details).

Current policies and procedures that align with the ADs would help the City ensure that general computer controls are executed consistently, job

responsibilities and accountability are properly assigned, and information technology processes are effectively managed.

Recommendation II

We recommend that the Director of CIS ensure that:

- Policies and procedures for change management, security administration, and computer operations are written and/or updated to reflect current CIS practices and that the policies and procedures align with the City's ADs
- ADs related to information technology are updated
- CIS standards and requirements are communicated to DPD and DFR information technology personnel

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

An Annual Review of Data Classification and Data Ownership Is Not Performed

The CIS does not perform an annual review of data classification and data ownership for DPD and DFR. Additionally, CIS does not provide a list of mainframe and network data files, for which CIS is the designated physical custodian, to the data owners (user departments) for verification. Per AD 2-25, *Data Classification and Ownership*, CIS is responsible for providing a list of mainframe and network data files on an annual basis so that the user departments can confirm the data classifications and the users who have access to the data.

In addition to complying with AD 2-25, a data classification and data ownership review would assist CIS in developing an applications inventory. An applications inventory is an essential element in information technology infrastructure planning, streamlining, and cost reduction. An applications inventory can also be used for: (1) policy/procedure analysis; (2) vulnerability analysis for risk management; (3) clarification of roles/responsibilities related to each application, such as back-up and security; and, (4) records retention management.

Definition of Data Classification

Data may be physically located within the departments in a variety of media or on the mainframe or corporate network computers. All data should be classified as one of the following:

Confidential – Either a mandatory or permissive exception to disclosure under the Texas Open Records Act. All access, at any level, must be approved by the Data Owner.

Production – Non-confidential data, i.e., that is not a mandatory or permissive exception to disclosure under the Texas Open Records Act, but which is deemed critical because of its importance to the organization and its operations. Update access is restricted and must be approved by the Data Owner.

Test – This is non-confidential, non-production data. Update access must be approved by the Data Owner.

Source: Administrative Directive 2-25, *Data Classification and Data Ownership*, Section 6.1, Page 3

An applications inventory would assist CIS and the user departments in:

- *Determining which set of data poses a higher risk to the City so that the data is adequately protected.* For instance both DPD and DFR have to comply with the *Criminal Justice Information Systems (CJIS)* security policies which include rigorous standards for maintaining data confidentiality for the CAD application. The National Fire Incident Reporting System (NFIRS), however, may not be required to follow such rigorous standards; therefore, this data would be considered lower risk.
- *Prioritizing systems issues and concerns that might occur during the normal course of operations, such as change requests.* For example, if DPD/DFR requests a change to the 24/7 Computer Aided Dispatch (CAD) application and a change request is also being completed for the Geographic Information System (GIS) (an application that holds all the

City's addresses and maps), a data classification would assist in evaluating if a change in GIS would impact the change request for CAD.

- *Confirming that the access to data is granted consistently on a need to know basis.* The CIS, DPD, and DFR often update their organizational structures resulting from various operational changes. As personnel move within a department or to another department, their need for access to data also changes. An annual review of the data owners would assist in verifying that access is limited and managed appropriately.
- *Identifying that data is appropriately backed-up and made available for recovery based on the classification schema.* The user departments process volumes of transactions each day; however, not all of the data that is processed would fall into a data classification category that requires regular back-up. For example, the DFR Locution application, which alerts fire stations of incoming calls, may not need to be backed-up at all. On the other hand, the DFR NFIRS application which records DFR incidents might require back-ups on a more regular basis.

Since the objective of the data classification and data ownership is that data is classified, data is protected according to the classifications, and access to data is managed, an applications inventory of all DPD and DFR applications that would address the AD requirements would assist CIS in effectively managing data.

Recommendation III

We recommend the Director of CIS review and update Administrative Directive 2-25 to reflect current standards for data management. We also recommend the Director of CIS develop an applications inventory for DPD and DFR to ensure that data is classified, protected according to the classifications, and access to data is properly managed.

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

Section II: Change Management

Changes to Data and Systems Do Not Comply with Administrative Directive 2-28, *Change Management for Information Technology*

Changes to data and systems are not always formally approved, planned, tested, and recoverable in accordance with the change management procedures stated in AD 2-28, *Change Management for Information Technology*. Instead, changes to data and systems, including emergency change requests, are completed in an ad-hoc manner. Additionally, there is not a periodic review of 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, CIS does not have a formal process in place to:

- Include all change events related to DPD and DFR in CIS's central repository, the Change Management Database (CMD). Without a complete central repository for DPD and DFR change events, CIS cannot perform a comprehensive impact analysis to ensure that prior change events and/or planned change events do not have conflicting objectives among user departments.
- Obtain and track user department approvals for change events. Tracking user department approvals helps to ensure that only appropriate and authorized changes to applications and hardware are made and that the changes are transparent to all parties involved.
- Prioritize and schedule change events. Prioritizing and scheduling change events helps to ensure that change events introduced into production do not result in processing errors or disruptions to business operations.
- Test change requests. Testing change requests helps to determine that: (1) the initial planned objectives are met; (2) the impact to other applications and their functionality is minimized; and, (3) to ensure an audit trail of user involvement exists to validate that the change request underwent the full extent of the testing before the change was placed into production.

Change management procedures that include formal processes for approvals, prioritization, testing, and impact analysis ensures that only those changes to data and systems which are critical to business operations are introduced into production. Additionally, change management controls would facilitate in

achieving data quality, minimizing post-production problems, and executing changes timely to meet business objectives. A well designed change management process could also increase efficiencies in the process and result in a more effective use of resources.

Recommendation IV

We recommend the Director of CIS comply with AD 2-28 by developing, documenting, and implementing formal change management procedures that are standard, reliable, and consistent so that only authorized, planned, prioritized, and tested changes are made to data and systems.

We also recommend the Director of CIS maintain a central repository of all change events.

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

Section III: Computer Operations

Data Backup and Restoration Processes Do Not Fully Comply With Administrative Directive 2-34, *Data Backup and Recovery, Standard, and Procedures for the Mainframe and Servers*

The CIS does not fully comply with AD 2-34, *Data Backup and Recovery, Standard, and Procedures for the Mainframe and Servers* for backup and restoration of DPD and DFR information technology components (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 the ability of DPD and DFR response and ability to serve the citizens. The objective of non-disaster data backup and recovery is so the City can continue to conduct business without interruptions.

Scheduling and Monitoring of Backups

The CIS Network Operations Center (NOC) schedules full daily backups for the mainframe applications, one CAD server, and one of the four CAD databases; however, CIS does not retain documentation to show how the errors in backup processing were resolved.

For example, the CAD application database audit log showed that in four of the 30 days tested, backups were not completed. The CIS could not provide documentation to explain why these four backups did not occur. If CIS had a formal monitoring process for both the mainframe and the client server applications, the four days would have been identified and the backup processing errors resolved.

Additionally, the DPD and DFR client server applications not supported by the NOC appeared to be scheduled for backup; however, there was no evidence that the backups were completed successfully or resolved.

Off-site Tape Rotation

The DPD mainframe applications and the CAD application backup tapes are not rotated off-site to an alternate location for non-disaster recovery purposes. As a result, if the tape management system where the backup tapes are located

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

malfunctions, there is currently no form of data retrieval for the DPD mainframe applications and CAD application data.

The CIS confirmed that mainframe data backup is completed daily and rotated off-site for disaster recovery purposes; however, CIS could not confirm that CAD data is handled in this manner. Although the off-site tape rotation for mainframe data is completed for disaster recovery purposes, this may not include the most recent production data which would be necessary in a non-disaster recovery event. For example, disaster recovery data retrieval may restore data from the prior day, but it may not include data for the most recent DPD production data.

Additionally, the remaining DPD client server applications (Criminal History, Police Manager, and Evidence Manager) as well as all the DFR client server applications have not been rotated to off-site tape. The Texas Administrative Code, Chapter 7, Rule 7.75 *Security of Electronic Records*, which is cited in AD 2-34, requires off-site storage of backup media so that the value of creating backups for future restoration and recovery is maintained.

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. Per the Texas Administrative Code, Chapter 7, Rule 7.76 *Maintenance of Electronic Records Storage Media*, which is cited in AD 2-34, backup media and the data on the media should be tested periodically so that it can be validated for recoverability. The NOC personnel stated users' requests to retrieve documents on the network drives that were damaged or lost were completed successfully; however, a user's requests for retrieval of documents on the network is not the same as restoration of data in the databases of critical systems.

Recommendation V

We recommend that the Director of CIS establish data backup and restoration procedures to abide by and comply with the minimum standards stated in AD 2-34 and the Texas Administrative Code Chapter 7, Rule 7.75 and Rule 7.76.

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

Appendix I

Background, Objective, Scope and Methodology

Background

In 2007, the Department of Communication and Information Services (CIS) was directed to centralize and manage all information technology functions across the City. Prior to 2007, the two public safety departments, the Dallas Police Department (DPD) and the Dallas Fire-Rescue (DFR), had independent information technology functions supported by each department's internal information technology groups. These information technology groups were responsible for procuring, safeguarding, and maintaining information systems and data. They were also responsible for ensuring that each department complied with applicable federal and state information technology general computer controls.

Progress Towards DPD and DFR Information Technology Centralization

As of July 2009, CIS was continuing to work with DPD and DFR to centralize and standardize certain information technology functions. The CIS had combined all network functions, for both DPD and DFR.

- **Some DPD Information Technology Functions Had Been Centralized**

The CIS had organizationally re-structured certain personnel to incorporate former DPD information technology personnel into CIS. Portions of the DPD information technology functions had also been integrated, such as access administration to the DPD Active Directory and sharing of some knowledge of the applications. Additionally, DPD information technology functions were completed by a combination of CIS and DPD personnel. There are, however, other areas, such as the computer operations (e.g., backups and off-site tape rotations), that are not centralized.

- **The DFR Information Technology Functions Remain Independent**

The DFR continues to maintain an independent information technology function since the DFR information technology personnel had not been organizationally re-structured and incorporated into CIS. The DFR also continues to use a different e-mail application than the City and manages its own applications, completes its own backup functions,

and administers security to all its applications including portions of the Computer Aided Dispatch (CAD) application.

Dallas Police Department's Information Technology Architecture

The DPD information technology architecture is a combination of mainframe and client server environments. The mainframe applications are Direct Entry Field Reporting Systems (DEFRS) and Direct Entry Arrest Reporting Systems (DEARS). The selected sample of DPD client server applications reside on stand-alone servers and are not integrated into either CIS or DPD's Active Directory structure. All of the applications that DPD uses are considered high-risk by CIS.

Dallas Fire-Rescue's Information Technology Architecture

The DFR information technology architecture is a client server environment only. The majority of the DFR applications are webpage applications and are designed to either look-up data or collect data via input. The DFR applications reside on stand-alone servers and are not integrated into the CIS Active Directory structure. All of the applications that DFR uses are considered high-risk by CIS.

Jointly-Owned Application – Computer-Aided Dispatch

The CAD is a jointly-owned application between DPD and DFR. The CIS department is responsible for the support and maintenance of the application. The CIS currently outsources portions of the support and maintenance of the application to the vendor. The data is owned by both user departments (DPD and DFR) and, therefore, the data integrity and confidentiality of the information in the application is the responsibility of both user departments.

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 2009 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 general computer controls for DPD and DFR. The scope of the audit covered the information technology areas of change management, security administration, and computer operations from February 2009 through July 2009. The DPD and DFR general computer controls are primarily administered by CIS. As a result, the evaluation included CIS.

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 control issues have been communicated to the appropriate CIS personnel in the *Limited Use Report – DPD/DFR Security Administration*.

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

- Reviewed existing policies and procedures and the City’s Administrative Directives (AD) 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 for DPD and DFR 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 DPD and DFR general computer controls for compliance with the City's ADs related to information technology and the control objectives as specified in CoBIT
- Interviewed CIS, DPD, and DFR personnel who support the DPD and DFR information technology infrastructure (mainframe, network, and client server environments), as well as the personnel who support the jointly-owned CAD application

Additionally, we completed a reasonableness analysis to determine which industry best practice 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.

Control matrices for security administration, change management, and computer operations were generated and shared with CIS 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
Kevin Hannigan, CIA – Auditor
Theresa Hampden, CPA – Quality Control Manager

Appendix III

Management's Response

Memorandum

RECEIVED

JUN 16 2010

City Auditor's Office



CITY OF DALLAS

DATE: June 15, 2010

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report: Audit of Selected Computer Controls for the Dallas Police Department and the Dallas Fire-Rescue Primarily Administered by the Department Of Communication and Information Services

Our responses to the audit report recommendations are as follows:

Recommendation I:

We recommend that the Director of CIS establish a general computer controls framework that aligns with best practices that are commonly used and accepted in the United States – such as CoBIT, and one that provides City Council, management, as well as the Office of the City Auditor and external auditors, a consistent means to evaluate whether general computer controls are improving.

We also recommend that the Director of CIS perform regular general computer control self-assessments to ensure that the general computer controls framework is designed and operating as intended.

Management Response / Corrective Action Plan

Agree Disagree

The CIS Department will establish a general computer controls framework to address Data Center Operations, Change Control, Computer Systems Control, Security Control and Application System Maintenance Controls. This will include self-auditing standards and procedures to ensure an annual review of all General Computer Control activities.

To ensure a consistent means to evaluate improvement of general computer controls CIS has developed a set of relevant process frameworks. As an example, CIS has developed an Incident Management process framework based upon the ITIL v3 best practice definition. The CIS Incident Management process framework has been communicated to operational teams through a twelve week series of workshops. Workshop participants discuss incident management under ITIL v3 and identify and discuss present challenges to incident handling within CIS. Upon completion of the Incident Management workshops, operational teams will define and implement incident management protocols for major services supported by CIS. This framework accommodates root cause analysis and will capture and measure incidents related to general computer control activities and their effectiveness.

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

**An Audit Report on –
Selected General Computer Controls for the Dallas Police Department and Dallas Fire-Rescue
Primarily Administered by the Department of Communication and Information Services**

CIS process frameworks will be reviewed annually for appropriateness and updated as required to meet departmental needs.

Implementation Date

March 31, 2011

Responsible Manager

Patricia Smith, William Walling and Rowland Uzu

Recommendation II:

We recommend that the Director of CIS ensure that:

- Policies and procedures for change management, security administration, and computer operations are written and/or updated to reflect current CIS practices and that the policies and procedures align with the City's ADs
- ADs related to information technology are updated
- CIS standards and requirements are communicated to DPD and DFR information technology personnel

Management Response / Corrective Action Plan

Agree Disagree

CIS is developing a Change Management process based upon best practice as defined in ITIL v3. Proper implementation of Change Management will drastically reduce or eliminate unauthorized change to deployed services, improve service delivery, and provide a known technology baseline for stakeholders.

CIS is presently disseminating information regarding ITIL v3 Change Management best practice to staff through a series of workshops. Process activities, process functions, and process flow are presently being discussed. Upon completion of the Change Management workshops, operational teams will negotiate and implement the Change Management process to meet the organizational need for controlled change.

CIS will also ensure that all ADs related to information technology are updated and communicated to DPD and DFR.

CIS process frameworks and Administrative Directives pertaining to information technology will be reviewed annually for appropriateness and updated as required to meet departmental needs.

Implementation Date

April 30, 2011

Responsible Manager

David Oldham, Patricia Smith and William Walling

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

**An Audit Report on –
Selected General Computer Controls for the Dallas Police Department and Dallas Fire-Rescue
Primarily Administered by the Department of Communication and Information Services**

Recommendation III:

We recommend the Director of CIS review and update Administrative Directive 2-25 to reflect current standards for data management. We also recommend the Director of CIS develop an applications inventory for DPD and DFR to ensure that data is classified, protected according to the classifications, and access to data is properly managed.

Management Response / Corrective Action Plan

Agree Disagree

The Data Management initiative within CIS presently focuses on data architecture, database operations, data quality, data security management, and data governance domains. Data management teams are developing complementary frameworks to achieve specified goals within each domain and to support the goals of related domains. Initial deliverables include data policies, standards, and governance processes. The overall goal of the Data Management initiative is to secure, protect, and manage the City's information base.

Governance: Annual Cycle

- Data Security Policy Review
- Data Operational Policy Review
- Data Quality Assessment
- Maintain Data Architecture models
- Periodic Review of Data Management Strategy

Implementation Date

March 31, 2011

Responsible Manager

William Walling

Recommendation IV:

We recommend the Director of CIS comply with AD 2-28 by developing, documenting, and implementing formal change management procedures that are standard, reliable, and consistent so that only authorized, planned, prioritized, and tested changes are made to data and systems.

We also recommend the Director of CIS maintain a central repository of all change events.

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

**An Audit Report on –
Selected General Computer Controls for the Dallas Police Department and Dallas Fire-Rescue
Primarily Administered by the Department of Communication and Information Services**

Management Response / Corrective Action Plan

Agree Disagree

CIS is developing a Change Management process based upon best practice as defined in ITIL v3. Proper implementation of Change Management will drastically reduce or eliminate unauthorized change to deployed services, improve service delivery, and provide a known technology baseline for stakeholders.

CIS is presently disseminating information regarding ITIL v3 Change Management best practice to staff through a series of workshops. Process activities, process functions, and process flow are presently being discussed. Upon completion of the Change Management workshops, operational teams will negotiate and implement the Change Management process to meet the organizational need for controlled change.

CIS is presently evaluating Change Management systems to ensure a single, centralized solution to track, automate, manage, control and report on the change and approval process.

The CIS Change Management process framework will be reviewed annually for appropriateness and updated as required to meet departmental needs.

Implementation Date

March 31, 2011

Responsible Manager

David Oldham

Recommendation V:

We recommend that the Director of CIS establish data backup and restoration procedures to abide by and comply with the minimum standards stated in AD 2-34 and the Texas Administrative Code Chapter 7, Rule 7.75 and Rule 7.76.

Management Response / Corrective Action Plan

Agree Disagree

CIS will create a policy to establish a backup strategy to address different types of service disruptions. The strategy will include Business Backup & Recovery Requirements, Schedules, Retention Standards, Backup Standards, Recovery Standards, Rotation Schedules, Off-Site Storage Services, Destruction Standards, Operation Control Policies & Procedures, and Verification Standards and Policies.

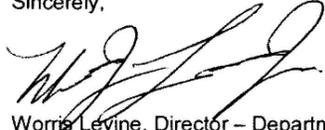
"Dallas: The City That Works: Diverse, Vibrant, and Progressive."

**An Audit Report on –
Selected General Computer Controls for the Dallas Police Department and Dallas Fire-Rescue
Primarily Administered by the Department of Communication and Information Services**

Implementation Date
December 31, 2010

Responsible Manager
Patricia Smith

Sincerely,



Morris Levine, Director – Department of Communication and Information Services

C:

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