

OFFICE OF THE CITY AUDITOR

AUDIT OF THE CITY'S MAINFRAME OPERATING SYSTEMS AND OPERATIONS



Paul T. Garner
Assistant City Auditor

Prepared by:

Tony Aguilar, CISA
Sr. IT Auditor

November 24, 2004

Memorandum



CITY OF DALLAS

November 24, 2004

Honorable Mayor and Members of the City Council
City of Dallas

We have conducted an audit of the City's data center, mainframe system, and operations.

The City has maintained a computing environment centered around the mainframe for many years. As the computing environment is becoming more decentralized using client server technology, the Communication and Information Services department will be challenged resource-wise and organizationally in meeting the operating requirements in both environments.

As a result of our inquiries, examinations, and reviews, we conclude that there are several factors that may affect critical public safety services.

Paul Garner

Paul T. Garner, CCP, CSP
Assistant City Auditor

c: Mary K. Suhm, Interim City Manager

**AUDIT OF THE CITY'S MAINFRAME OPERATING SYSTEMS
AND OPERATIONS**

CONTENTS

	<u>PAGE</u>
EXECUTIVE SUMMARY	1
INTRODUCTION	2
Authorization	2
Scope and Methodology	2
Overall Conclusion	2
Background	3
OPPORTUNITIES FOR IMPROVEMENT	4

EXECUTIVE SUMMARY

We have conducted an audit of the City's data center, mainframe system, and operations. As a result of our inquiries, examinations and, reviews, we conclude that processes and procedures can be improved to enhance the efficiency and the effectiveness of the operations reviewed. We reviewed Communication and Information Services' organizational structure, assessed quality assurance procedures and workforce strategic planning efforts, and reviewed preventive maintenance requirements on data center equipment. We also cite organizational changes that should be considered to improve the efficiency and effectiveness of service delivery.

We have summarized our opportunities for improvement below.

- The assignment of operational responsibilities within CIS' current organizational structure appears to be causing operational inefficiencies or service gaps.
- Although controls exist for the change notification process, current procedures are not adequate to ensure a consistently high level of quality in the software development process.
- Lack of effective strategic planning may result in areas of workforce composition, succession, training, and software application technology not being aligned with future needs.
- Preventive maintenance is not adequate on key operational equipment for the data center and places unnecessary risk on critical City operations.

Also, the current tape inventory in the data center is inadequate.

INTRODUCTION

Authorization

We have conducted an audit of the City's data center, mainframe operating systems and operations. We conducted this audit under the authority of Chapter IX, Section 2 of the Dallas City Charter and in accordance with the Annual Audit Plan approved by the City Council.

Scope and Methodology

We performed our audit in accordance with generally accepted government auditing standards and included tests and other procedures that we considered necessary in the circumstances.

Our audit covers the period from July 25, 2003, through April 30, 2004.

The audit objectives were to:

- Evaluate environmental controls that reduce the risk of damage to the data center computer equipment from a disaster, such as a fire or flood;
- Evaluate security controls designed to prevent and detect unauthorized logical and physical access to information on computer systems;
- Evaluate hardware and system software maintenance procedures to ensure all changes are authorized, approved, and tested; and
- Evaluate the segregation of duties within the data center to ensure that it is adequate.

This audit included activities of the Communication and Information Services (CIS) and Equipment and Building Services Departments (EBS).

Due to public safety and privacy concerns, the audit objective addressing security controls has been omitted from this report. Our decision to exclude this information is based on the Government Auditing Standards, June 2003, Sections 8.35, 8.36, and 8.37. Our findings pertaining to security controls have been communicated to the appropriate information security personnel.

Overall Conclusion

As a result of our inquiries, examinations, and analyses, we conclude that processes and procedures can be improved to enhance the efficiency and the effectiveness of the operations reviewed. We also cite organizational changes that should be considered to improve the efficiency and effectiveness of service delivery. Due to the limited amount of time remaining for the audit, we did not review segregation of duties in the data center and

INTRODUCTION

will address this objective in a future audit.

We found that controls exist within the Applications Development area of CIS to ensure that the change notification process is performing satisfactorily.

To develop an understanding of the mainframe and to identify any organizational, system, or operational issues, we reviewed the following:

- CobiT (Control Objectives for Information and Related Technologies)
- Administrative Directive 2-28, 2-29, 2-30, 2-34
- Data Center Employee Manual
- LINC (Lane Information Network Controller) Systems Programmer's Guide
- Information Systems Manual – Volumes 1 & 2
- CIS Data Center Training & Standards Manuals
- CIS Organizational Charts, Procedures, and Software Testing Procedures
- Hardware, Software, and Maintenance Contracts
- Capability Maturity Model Integration (CMMI), Version 1.1
(<http://www.sei.cmu.edu/publications/documents/02.reports/02tr028.html>)
- CIS Proposed Strategic Direction for 2000-2005
- Rothman Consulting Group – Study on Developer/Tester Ratios
- GAO Audit Report: "Key Principles for Effective Strategic Workforce Planning", December 2003

Background

The data center housing the mainframe was part of the construction of the new City Hall in the 1970's. From that time and into the 1980's, the mainframe served the City as the primary source of data processing resources. Based on an inventory provided by data center personnel, the data center currently houses approximately 200 pieces of hardware that support mainframe and client/server technologies. The single Fujitsu mainframe is supported by approximately 95 units of supporting hardware. For client server technologies, more than 100 servers are housed in the data center.

As technology progressed in the 1990's, the data center implemented distributed processing, which resulted in programs being shifted to client/server technologies. Additional equipment, cabling, and power requirements were added to the data center to accommodate the client/server technology.

A major development in the service delivery mission of CIS was an information technology (IT) resource consolidation in Fiscal Year 2001. In that consolidation, funding for 76 full-time positions was transferred from various departments to CIS. This action dramatically expanded the scope of responsibilities for CIS. The consolidation also added a requirement to re-shape an organizational structure that would be designed to provide

INTRODUCTION

quality computer services to all City departments.

OPPORTUNITIES FOR IMPROVEMENT

We identified certain policies, procedures, and management practices that can be improved. Our audit was not designed or intended to be a detailed study of every relevant system, policy, and transaction. Accordingly, the opportunities for improvement presented in this report may not be comprehensive of the areas where improvements may be needed.

1. The assignment of operational responsibilities within CIS' current organizational structure may be causing operational inefficiencies or service gaps.

Responsibilities for certain operations may not be assigned and grouped according to operational expertise and may be negatively affecting operational issues. The risk of this condition to the City is that functional requirements may not be achieved if conflicting definitions of operational responsibilities are not clarified between CIS divisions.

We reviewed the operational areas within CIS to determine if the organizational structure in place effectively addresses the current and future needs of the City. As the City evolves from a mainframe centric organization to a distributed processing environment, it is important that CIS resources are aligned to address and structurally support the implementation of client-server technologies. Departments are using a strategy of replacing long-standing mainframe programs with applications operating on departmental servers. This strategy is particularly being pursued on LINC programs. Although the mainframe will continue to be the platform of choice for certain applications, our analysis indicates that operational efficiencies may be sacrificed if changes to the current organizational structure are not implemented.

While structures may vary from organization to organization, albeit public or private, one consistent pattern emerges that provides the foundation for future growth; that clear, distinct, and logical lines of responsibility within the organization are developed.

The Information Systems Audit and Control Foundation has developed a document, which establishes standards for implementing Information Technology (IT) governance. According to COBIT, IT governance is:

“A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.”

It also states:

OPPORTUNITIES FOR IMPROVEMENT

“IT governance provides the structure that links IT processes IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalizes good (or best) practices of planning and organizing.”

Section PO4 of COBIT, “Define the Information Technology Organization,” reviews the IT organization and relationships that are necessary for IT to deliver the right services. It states that control over the IT process is enabled by an organization that is suitable in numbers and skills,...is aligned with the business; and that facilitates the strategy and provides for effective direction and adequate control, and takes into consideration:”

- Management’s direction and supervision of IT
- IT’s alignment with the business
- Organizational flexibility
- Clear roles and responsibilities
- Staffing levels and key personnel
- Organization positioning of security, quality, and internal control functions

In further applying COBIT principles in our review of the CIS organizational structure, we analyzed CIS in terms of broad areas of responsibility and functional-specific tasks within each broad area. The CIS organization is divided into three areas. These areas include:

- Information Services
- Communication
- Business Management

A breakdown of the responsibilities of each area is shown in Table 1 (next page). The table lists the major functional areas within CIS such as Web Development programming, Database Administration, Quality Assurance; and it identifies the area with which they are currently aligned. The color bars indicate whether the function is appropriately aligned within the organizational structure. For example, note that the Data Backup function is a subset of the Systems Programming area and falls under the “Information Services” column. We have assigned a red color to this function to indicate that the Data Backup function is misaligned to the Systems Programming area because it is actually a function of operations instead of programming.

OPPORTUNITIES FOR IMPROVEMENT

Table 1
Functional Responsibilities within Current Organizational Structure

-  Function does not match organizational structure
-  Function is consistent with organizational structure
-  Function is independent in nature

Area (Based on CIS organization chart)	Function	Information Services (Chuck Mumm)	Communication (Bill Finch)	Business Management (Teresa Page-Davis)
Data Center	Help Desk			
	Computer Operations	☒		
	Tape Library			
	Report Distribution			
Applications Programming	Web Development			
	Mainframe			
	Distributed Systems			
Systems Programming	Database Administration			
	eMail	☒		
	Windows Server	☒		
	Directory Services			
	Novell Server			
	Data Backup			
	O/S 390			
	MVS			
	LINC			
	MDT (DPD, DFD)	☒		
Network Operations	Radio			
	VoIP			
	Infrastructure			
CIS Security	Physical	☒		
	Logical			
Business Administration	Finance/Accounting			
	Project Management			
	Change Management	☒		
	Quality Assurance	☒		
	Disaster Recovery	☒		

OPPORTUNITIES FOR IMPROVEMENT

α - See Table 2 for examples

Based on the organizational alignment as shown in Table 1, we observed areas of risk in the current organizational structure. Examples are shown in Table 2:

**Table 2
At-Risk Conditions of Current CIS Organizational Structure**

CONDITION	RISK	CAUSE
Communication services, such as email and directory services report under Systems Programming.	Implementation of Outlook has not included a review of the effect of the implementation on network and desktop support issues.	System Programming staff have ability to drive technical direction of telecommunication and messaging areas.
Server configuration/maintenance that reports under AD who is also responsible for Applications Programming.	The most appropriate technical solution for a problem may be excluded from consideration based on existing technical expertise.	Strategic direction in the areas of hardware and operating systems may be unduly influenced by platform independent application development group. Example: Prior CIS Assistant Director of Applications Programming set hardware technical direction by excluding the Unix operating system from the City. This action effectively eliminated potential application solutions from consideration.
MWS servers ownership is undefined.	Security and maintenance may experience lapses in oversight.	Ownership of the servers has not been firmly established.
Change Management that reports to Business Management.	Decision-making capabilities, strategic planning, and technical requirements may not be adequately addressed and fully comprehended.	Technical and operational functions are misaligned under a business management role.
Quality Assurance that reports to Business Management.	Decision-making capabilities, strategic planning, and technical requirements may not be adequately addressed and fully comprehended.	Technical and operational functions are misaligned under a business management role.
Disaster Recovery that reports to Business Management.	Management may lack the necessary technical support skills to effectively respond to IT crisis situations.	Technical and operational functions are misaligned under a business management role.

As CIS has downsized staffing resources over the last few years, functional areas have been reassigned to other areas to maintain operations. As a result, certain functional areas may lack the overall management oversight and technical expertise necessary to fully support the operational area.

We recommend that the Chief Information Officer (CIO):

OPPORTUNITIES FOR IMPROVEMENT

- A. Conduct an analysis focused on matching the appropriate alignment of functional tasks to organizational hierarchical responsibilities within CIS.
- B. Develop and implement a plan to execute the results of the organizational analysis performed in A. above.

Management's Response:

- A. CIS agrees. CIS will conduct an analysis of critical business functions, tasks and organizational structure.

(Refer to Table 2 – Page 24 for discussion of Item 2, 3, and 4)

Item 2: CIS does not concur with the Risk or Cause as stated here.

- A. Email: The general (commercially) accepted term for email is groupware, not communication services. Unlike telephone, email system requires programming, much, much deeper user administration, monitoring, and data retention. In fact, email data retention falls in the data life cycle. The same cannot be said about telephone. With the implementation of VoIP, the functionalities and capabilities of email to manage voice is being exploited but not the other way around. Email deployment has been a joint project between Server Support and Desktop Support. The HEAT system is used to coordinate the installation of the email client software and migration of user email data. The Server Support staff would step in only if there is a problem that Desktop staff cannot resolve. The Network impact of the deployment of Outlook is no different than with Groupwise. In fact, the Outlook client has a lower network impact due to the limit of email size of 4 megabytes. With Exchange, there is a user mail box limit of 25 megabytes. GroupWise has no such limit, for example, users were caught sending one email with half-a-gigabyte attachment which used up a lot of network bandwidth and filled up the email server.
- B. Directory Services: Directory Services impact the areas of Security, Server Support, Desktop Support, and at a much lesser degree, Network. The highest controlling group for this activity should be CIS Security, which should then delegate appropriate controls, accesses and permissions to the Server Support and Desktop Support groups. All three groups ARE working together to make this happen.

Item 3: CIS does not concur with the Risk or Cause as stated here. Technical Bias does not exist. Three (3) years ago, with no CIS staff with any UNIX experience,

OPPORTUNITIES FOR IMPROVEMENT

CIS had to draw the line to support what it could. Now CIS has three (3) staff members trained in supporting UNIX and has obtained approval from the Council to acquire Sun Cluster equipment to upgrade CRMS. CIS will continue to seek "best of the breed" solutions, if supportable. But CIS will continue to be cautious of embracing technologies that it cannot support.

Item 4: See previous discussion pertaining to page 15, about administration of the MWS Servers.

B. CIS agrees and will implement acceptable organizational changes, as budget permits.

2. Although controls exist for the change notification process, current procedures are not adequate to ensure a high level of quality in the software development process.

A. Software code review process does not follow industry-standard guidelines.

CIS has not adopted any industry-standard process improvement models according to a Sr. IT Manager in applications programming. One of the primary process improvement models is the Capability Maturity Model Integration (CMMI-SW), Version 1.1, published by the Carnegie Mellon Software Engineering Institute (SEI). This model is a tool that helps organizations improve their processes. According to the CMMI, software testing and peer review are integral parts of the application development lifecycle. The CMMI describes two approaches to software testing:

- 1) Testing by an independent group (usually Quality Assurance)
- 2) Testing performed by peers

A peer review is the review of a person's work performed by peers during development of the work products to identify defects for removal. According to the CMMI, Version 1.1, page 70, "Peer reviews are a proven method for removing defects early and provide valuable insight into the work products and product components being developed and maintained."

CIS procedures, as outlined in Sect. III.D.1, Change Control, page 8, item 4, state that:

OPPORTUNITIES FOR IMPROVEMENT

- 1) "Programmers are responsible for following this procedure, and for **testing all updates to the Production Environment thoroughly** before moving them to production.
- 2) "Managers are responsible for assigning projects to programmers, for reviewing the work, and for **assuring that testing has been completed** before the code or JCL is moved to production."

Section III.D.1, page 4, last paragraph of the "Definitions" section states:

- 3) "This is the document by which the client who requested the change to the system indicates that the change has been completed to his/her satisfaction, **that testing has verified the accuracy of the changes**, and that he/she is ready for the program to be moved into the production environment."

To summarize, the CIS process for testing and approving code means that:

- 1) Programmers test their own code.
- 2) Managers are to ensure that programmers test their own code.
- 3) Client departments perform testing.
- 4) An independent entity does not perform quality assurance testing.

When compared to the CMMI standards, the CIS procedures are shown to be deficient as presented in Table 3:

**Table 3
Code Review Guideline Comparison**

Guideline	CIS	CMMI
Initial code review by system analyst	Yes	Yes
Code testing		
- Independent review	No	Yes
- Qualified peer review	No	Yes
- User Acceptance	Yes	Yes

CMMI provides a secondary option for those development organizations desiring to maintain high-quality standards, but not employ the use of an independent software quality assurance group.

CMMI-SW, page 465, states: "Objectivity in process and product quality assurance evaluations is critical to the success of the project. Objectivity is achieved by both independence and the use of criteria. Traditionally, a quality assurance group that is independent of the project provides this objectivity."

OPPORTUNITIES FOR IMPROVEMENT

CMMI-SW also states: "It may be appropriate in some organizations, however to implement the process and product quality assurance role without that kind of independence. For example, in an organization with an open, quality-oriented culture, the process and product quality assurance role may be performed, partially or completely, by peers; and the quality assurance function may be embedded in the process."

The CMMI reference to "peer review" is qualified by the following CMMI statement on page 465: "If quality assurance is embedded in the process, several issues must be addressed to ensure objectivity. Everyone performing quality assurance activities should be trained in quality assurance."

CIS follows this secondary testing methodology, but according to a Sr. IT Applications Programming Manager, none of the programmers are trained in quality assurance. Since they are not properly trained to perform a quality assurance function, CIS is not completely adhering to the CMMI guidelines for performing quality assurance. The risk to the City is that more errors may be encountered after code is moved into a production environment. The effect of the higher error rate is to 1) delay the project's implementation, and 2) incur costs to the City to fix the malfunctioning code.

B. Measurement tools are not in place to gauge the quality of the software development process.

According to the Sr. IT Applications Programming Manager, CIS does not track defects nor does it employ any tools to measure or track the quality of code that is produced. Without the use of tools, it is difficult to measure the quality and efficiency of the individual programmers and of the development projects themselves.

There are many quality improvement tools that can be employed to increase the quality of code produced and minimize the number of errors generated. These tools include check sheets, charts, diagrams, histograms, and others. One of the basic metrics used to monitor the quality of programming efforts is "defects". Defects refers to the number of errors or defects encountered in the code. Defects can be tracked by day, week, month, project, development stage, or system analyst. They provide the means to measure progress on a project and to determine where problems may be developing on a project.

We reviewed two industry sources to determine some of the more common management tools being used to monitor and report on software development

OPPORTUNITIES FOR IMPROVEMENT

quality. These sources included the CMMI-SW (previously referenced) and a reference entitled Improving Software Quality, An Insider's Guide to TQM, John Wiley & Sons, 1993. TQM means Total Quality Management.

The Insider's Guide describes seven quality improvement tools that can be used in software development to improve the quality of the development process (page 80). These tools include:

- Check sheets – manual method of reporting total defects.
- Pareto charts – helps to focus energies on the areas that are causing the most problems.
- Ishikawa diagrams – identifies the causes of a problem and its root cause.
- Graphs – visual representation of the status of various performance measurements such as defects by week or defects by type.
- Histograms – help to depict the distribution of data by grouping information into “buckets.”
- Control charts – help to determine whether a process is “statistically” in control or wildly gyrating (uses data from different sources).
- Scatter diagrams - helps identify the relationships between two variables, such as the size of a program (lines of code) and how long it runs.

The CMMI-SW model (page 300) describes the requirement for defining and documenting measurable quality and process-performance objectives for a project. Project attributes for which metrics can be developed include:

- Percentage of defects removed by product verification activities such as peer reviews and testing
- Defect escape rates
- Number and density of defects (by severity) found during the first year following product delivery or start of service
- Cycle time
- Percentage of rework time

The quality and efficiency of code production is dependent upon the ability to capture data and present the data in a format that is meaningful and useful to the development team. For CIS, the absence of these tools means that:

1. The quality of a programmer's code is not being accurately measured, evaluated, or tracked over time.
2. Resource planning is hindered.
3. The ability to isolate coding problems is greatly reduced.

OPPORTUNITIES FOR IMPROVEMENT

4. The ability to determine the overall software development efficiency of a project is reduced.
5. Overall quality of a project can be negatively impacted.

We recommend that the CIO:

- A. Review and adopt the software review process as outlined in the CMMI-SW, Version 1.1.
- B. Implement the use of software measurement tools to monitor the progress and quality of all created and modified code.

Management's Response:

- A. CIS agrees. CMQA has documented a process to bring CIS more in line with industry standard practices by implementing formal testing processes.

CMQA is reviewing options to address the issues regarding testing and assessment of CIS' current processes to see whether CIS is regarding the CMMI-SW maturity model.

CMQA has also submitted a BAF for FY 2004-2005 to address the cost of implementing these processes.

- B. CIS agrees. CMQA makes use of the several quality improvement tools when the data is available for analysis. Data for the metrics listed in the audit are not captured by CIS, or is not captured as part of the processes in place. CMQA is developing a process based on current CIS procedures to include capturing the data needed to produce the metrics. This will include defects found at various points in the life cycle. CMQA is drafting the forms that will be used to document the defects found.

3. Lack of effective strategic planning may result in areas of workforce composition, succession, training, and software application technology that are not responsive to future needs.

A. Workforce planning does not address the future needs of critical systems.

A review of employees and their roles in supporting the mainframe revealed that a plan does not exist to provide programmer continuity in the event that key employees leave the City or are unable to perform their jobs. Two out of five mainframe staff are eligible for retirement in approximately two years^[c2]. According

OPPORTUNITIES FOR IMPROVEMENT

to the Sr. IT Manager responsible for mainframe programming, a resource continuity plan does not exist to address the future needs of the department. Our review of key systems and their resources indicates that two positions are particularly critical to mainframe operations. One of the positions is acutely important in nature. These key positions include:

- LINC programmer
- MVS programmer

The LINC position is of critical importance since many key systems (including Public Safety) operate on the LINC system. LINC is a proprietary system and has approximately 30 applications running on it. Some of these applications include:

- Fire Dispatch Support System
- Fire 9-1-1 Support Systems
- Police Dispatch
- Police Crime Analysis
- Geographic Information Systems (Street Services, Police, Fire, Building Inspection)

The City obtained the LINC software from Lane County, Oregon in the early 1970's. Over the years, the system was highly modified and maintained by a number of individuals. That number eventually dwindled to one person. This person retired from the City in 2002. CIS hired a systems programmer to be a backup to the LINC application programmer, but when he retired, the position was not filled due to a lack of funding. The current systems programmer believes he possesses sufficient knowledge to maintain the system on a day-to-day basis. On occasion, he seeks the advice and guidance of the retired City employee. The current systems programmer also stated that there are not any other programmers on staff possessing sufficient knowledge of the system to effect major repairs, if needed. When we interviewed other mainframe staff, we discovered that two other individuals possess some working knowledge of LINC, but only on a very limited basis.

Critical Dallas Police Department (DPD) and Dallas Fire-Rescue (DFR) systems currently operate on the LINC system. Although efforts are underway to move DPD and DFR applications off the mainframe, the City is at risk if the current LINC systems programmer were to leave the City or were unable to perform his duties. This risk level is heightened if access to the retired employee were also unavailable. If both events were to occur simultaneously, the City would have a difficult time ensuring system availability. It is important that support for major systems have

OPPORTUNITIES FOR IMPROVEMENT

sufficient primary and secondary programming resources to provide for business continuity, particularly where public safety systems are involved.

The second position at risk is a programmer who maintains the tape system. As with the LINC system, there is only one programmer on staff who possesses in-depth knowledge of certain key systems that run under MVS. These systems include the virtual tape system and the BMC Software suite of products. This programmer is eligible for retirement in approximately two years. No plans have been developed to provide backup programming responsibilities. As with the LINC systems programmer, the City is at risk if the MVS programmer were to leave the City or were unable to perform their duties.

According to a General Accounting Office (GAO) report entitled "Key Principles for Effective Strategic Workforce Planning," strategic workforce planning should address two critical needs:

1. Aligning an organization's human capital program with its current and emerging mission and programmatic goals, and
2. Developing long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals.

Additionally, the GAO report identified five key principles to address strategic workforce planning:

- Involve top management, employees, and other stakeholders in developing, communicating, and implementing the strategic workforce plan.
- Determine the critical skills and competencies that will be needed to achieve current and future programmatic results.
- Develop strategies that are tailored to address gaps in number, deployment, and alignment of human capital approaches for enabling and sustaining the contributions of all critical skills and competencies.
- Build the capability needed to address administrative, educational, and other requirements important to support workforce-planning strategies.
- Monitor and evaluate the agency's progress toward its human capital goals and the contribution that human capital results have made toward achieving programmatic results.

OPPORTUNITIES FOR IMPROVEMENT

B. Strategic planning does not adequately address the migration from legacy applications to new technologies.

There is not a formal and coordinated citywide effort to determine which applications should be moved off the mainframe and which applications should remain on the mainframe.

The City currently runs approximately 55 applications on the mainframe. Thirty applications run under the LINC operating system and 25 applications run under the IBM MVS operating system. Of the 30 applications on LINC, 10 are considered mission-critical. These mission-critical systems are an enabling factor in the delivery of public safety police and fire services to the citizens of Dallas. Efforts are currently underway at DPD and DFR to migrate applications from the LINC system to a client server-based environment.

A CIS document entitled "Proposed Strategic Direction for 2000-2005" states:

"The City of Dallas and CIS must make replacement of all LINC-based systems the number one priority for technology expenditures in the City."

It also states: ". . . due to technological and staffing issues, all LINC systems must be migrated to industry-standard platforms during the next five to seven years." However, according to the Sr. IT Applications Programming Manager, a migration plan does not exist to address the replacement issue. The strategic direction document was published in 1999. Its purpose was "to scrutinize the functions that have a significant impact on City operations" and to identify opportunities and make recommendations for both CIS and the City as a whole.

The challenge facing CIS is that with departments being the owners of the applications, CIS is not in a position to require those departments to migrate their applications to more technologically advanced platforms. CIS provides the resources to implement a new system, but since the departments provide the funding for each system, CIS cannot unilaterally force a strategic direction for each department.

The risk to the City of not having an executed migration plan is to perpetuate problems in supporting the proprietary LINC operating system and applications.

We recommend that the CIO:

OPPORTUNITIES FOR IMPROVEMENT

- A. 1. Provide funding to allow a backup LINC programmer to be hired or trained.
- 2. Adopt the five principles for workforce planning as specified in the GAO report.

Management's Response:

- A. 1. CIS agrees. CIS will implement this recommendation, as budget permits. Contingency, subject to funding authorization, will include hiring a consultant (Harold Nogle) to provide the training.
- 2. CIS agrees. CIS will implement this recommendation, subject to funding authorization.

We recommend that the City Manager:

- B. Empower ITEC (Information Technology Executive Committee) with decision-making authority to establish, adopt and enforce a strategic technology direction for the City.

Management's Response:

- B. CIS agrees. This recommendation is currently in place.

4. Preventive maintenance is not adequate on key operational equipment for the data center and places unnecessary risk on critical City operations.

Our review identified three key areas where maintenance has been deficient.

- A. **Contracts and maintenance agreements for the Uninterrupted Power Supply (UPS), back-up battery systems, back-up power generators, and electrical switchgear were cancelled.**

In September 2001, the City cancelled three separate vendor contracts that provided preventative maintenance for City Hall's emergency back-up power systems. A separate emergency back-up power system for DPD and DFR operations housed in City Hall was also cancelled. As of April 15, 2004, the contracts have not been renewed. The cancelled contracts are listed in Table 4:

Table 4
Cancelled Vendor Preventative Maintenance Contracts

OPPORTUNITIES FOR IMPROVEMENT

Contracted Vendor	Covered Equipment & Service Provided	Contract Term	Contract Cost (Not To Exceed)	Annualized Cost
Shermco Industries, Inc.	Electrical Switchgear <ul style="list-style-type: none"> • Preventive Maintenance • Remedial Maintenance 	60-months	\$502,695.00	\$100,539.00
			\$ 50,000.00	\$ 10,000.00
Powerware Global Services	UPS (Uninterrupted Power Supply) <ul style="list-style-type: none"> • Preventive & Remedial Maintenance 	60-months	\$124,164.00	\$ 24,832.80
Stewart & Stevenson Services, Inc.	UPS Generators <ul style="list-style-type: none"> • Preventive Maintenance • Remedial Maintenance 	60-months	\$ 62,281.00	\$ 12,456.20
			\$ 25,000.00	\$ 5,000.00
Total Maintenance			\$764,140.00	\$152,828.00

The determination to cancel the preventive maintenance contracts for both emergency back-up systems was deemed by CIS management as a necessary budget cut to reduce costs for the FY 2001-2002 budget. Upon inspection of the UPS, battery rooms, power generators and electrical switchgear, we found some of the batteries for DPD and DFR services (911) showing visible signs of corrosion on the battery posts. In the event of an emergency, complete power may not be available if some of the batteries are inoperable, thereby potentially affecting the delivery of 911 services.

EBS is responsible for the day-to-day building operations for City Hall. Emergency equipment requires a periodic inspection and preventive maintenance to ensure the City can continue operations during an emergency.

B. The contractor responsible for maintenance of the fire suppression system in the data center has not performed a test on the system.

The fire suppression system in the data center is at risk due to a malfunctioning sensor. According to an EBS Supervisor, the malfunctioning sensor may trigger an unplanned release of Halon gas if a complete system test were performed. The supervisor has indicated that the contractor will not perform a test of the system because of the malfunctioning sensor.

OPPORTUNITIES FOR IMPROVEMENT

The fire suppression system is based on Halon; a gas which removes enough oxygen from the air to prevent ignition of a flame. When a fire is detected, Halon gas is dispersed into the data center, thereby preventing the spread of a fire. EBS said that the vendor has not been able to identify and isolate the malfunctioning sensor. To ensure adequate safety measures are in place, each sensor should be tested on a periodic basis.

It should be noted that under the price agreement, the vendor is required to perform the necessary maintenance to ensure that the system is working according to specifications.

C. Cable runs in the data center raised-flooring are not adequately maintained.

Excess installation of cabling in some areas of the raised-floor in the data center has restricted airflow to computer equipment. When airflow is restricted, heat buildup occurs, which can cause damage and/or equipment failure.

In the data center, cabling for the mainframe, servers, communication equipment, and other types of equipment is located beneath the raised-flooring. In addition to distributing the cool air, the raised-flooring also provides safety and security for the cabling. During a walkthrough of the data center, the data center manager removed some floor tiles for our inspection. Most of the open panels we inspected were completely full of various types of cable. We inquired as to whether all of the cabling was still in use. The data center manager told us that much of the cabling was not being used. Under one of the floor tiles inspected, the cabling was so dense, that we could not feel any cool air coming up from the floor. The data center manager explained that the "unofficial protocol" or practice for installing cable was to place it on top of the existing cable.

The result of leaving inactive cabling in the raised-floor also limits or prohibits a number of maintenance tasks as follows:

- Addition or replacement of new cable runs.
- Removal of inactive cable runs.
- Troubleshooting cabling problems.
- Routine cleaning of the raised-flooring.

Maintenance of the raised-flooring is an industry practice instituted to ensure that:

- An unrestricted airflow is supplied to the equipment on the floor.

OPPORTUNITIES FOR IMPROVEMENT

- Adequate space is available to add new cable runs.
- Inactive cable runs are removed.
- Adequate space to perform repairs is available.

We recommend that the CIO:

- A. Renew support and maintenance agreements for all the components of the City's emergency UPS back-up systems.
- B. Enforce the testing provisions of the fire suppression system maintenance contract.
- C. Develop and implement a plan to identify and remove unused cabling in the raised-flooring.

Management's Response:

- A. CIS agrees. Three (3) systems maintenance/tests for the UPS are scheduled for 2004. Maintenance by Stewart and Stevenson has been completed. Maintenance by Powerware Global has begun but is not yet completed. Testing by Shermco is to be scheduled for an August date.
- B. CIS agrees. CIS is currently in the process of developing a plan to test the fire suppression system and to determine the best methods to mitigate any consequences that might result from performing a test of this system.
- C. CIS agrees. A Budget Adjustment Form has been submitted for FY 2004-2005 to address this situation.