
OFFICE OF THE CITY AUDITOR

AUDIT OF THE PROCEDURES GOVERNING THE LOCAL AREA NETWORK AND THE WIDE AREA NETWORK

**Thomas M. Taylor, CPA
City Auditor**

Prepared by:

Paul T. Garner, CCP, CSP
Senior Audit Manager

Anthony Aguilar
Senior IT Auditor

Thomas Ng, CPA, CISA
IT Auditor

**April 3, 2002
Report No. 357**

Memorandum



CITY OF DALLAS

April 3, 2002

Honorable Mayor and Members of the City Council
City of Dallas

We have conducted an audit of the procedures governing the Local Area Network and the Wide Area Network.

If correctly implemented, the recent consolidation of the administration and management of the City Local Area Networks can have a positive impact on the efficiency and effectiveness of delivering City services while reducing the cost of City operations. However, much work is needed in defining and implementing standards for the operation and maintenance of the network infrastructure as well as the training and support requirements to position the City's Communication and Information Services staff to meet the new computing environment challenges. Related opportunities for improvement and recommendations are presented in this report.

We appreciate the cooperation shown by City staff during our examination.

Thomas M. Taylor, CPA
City Auditor

c: Teodoro J. Benavides, City Manager

**AUDIT OF THE PROCEDURES GOVERNING THE LOCAL AREA NETWORK AND
THE WIDE AREA NETWORK**

CONTENTS

	<u>PAGE</u>
EXECUTIVE SUMMARY	1
INTRODUCTION	2
Authorization	2
Scope and Methodology	2
Overall Conclusion	3
Background	4
OPPORTUNITIES FOR IMPROVEMENT	5

EXECUTIVE SUMMARY

We have conducted an Information Technology audit of the Communication and Information Services (CIS) process and procedures governing the City of Dallas Local Area Network (LAN) and Wide Area Network (WAN).

As a result of our inquiries, examinations, and tests, we conclude that CIS has opportunities for improving the administration and management of the City's Local Area and Wide Area Networks as a result of the recent consolidation of these networks under CIS. We have summarized our major findings below.

- Multiple operating systems pose significant challenges in providing adequate service, support, and network performance monitoring. The existing computing environment consists of multiple operating systems on workstations and networks. This environment poses significant challenges in providing adequate support for network operations and workstations. Training standards for technical support need to be defined to operate and maintain a multiple operating environment. Additionally, department user training needs should be defined so that management can target training to meet the skill set requirements.
- LAN/WAN operational policies and procedures have not been fully defined and implemented. The LAN/WAN policies and procedures should be defined and implemented in the areas of disaster recovery, change management, software inventory, software distribution, and software license verification. Well-defined policies and procedures should provide an increase in operational efficiencies, reduce data security risks, and minimize legal liabilities to the City.
- Prior physical and logical data security issues remain unresolved. CIS has assessed the data and physical security needs, but adequate funding has not been committed to implement the plan. Data security risks and issues still exist due to uneven monitoring, lack of security software, and inadequate user training on data security.

We commend the department for accepting our recommendations and taking steps during the course of the audit to address these issues.

INTRODUCTION

Authorization

We have completed an audit of the procedures governing the Local Area Network (LAN) and the Wide Area Network (WAN). This audit was conducted 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, accordingly, included tests of records and other procedures that we considered necessary in the circumstances.

The objectives of our audit were to determine the adequacy of the administration and management of:

- Environmental and physical security procedures and controls
- Data security procedures and controls
- LAN/WAN operational procedures and controls
- Disaster recovery procedures and controls
- Change management controls
- Help Desk operations and performance
- Software distribution
- Network monitoring
- Computer login
- Service request system usage procedures
- Customer service efficiency
- Use of multiple operating systems

Our audit covered October 1, 2000, through December 31, 2001, and included all LANs in Communication and Information Services (CIS) and the following departments: Dallas Fire Department, Dallas Water Utilities, Dallas Police Department, Department of Public Works and Transportation, Department of Street Services, and the Dallas Public Library. In addition, the audit included mainframe systems, the City WAN systems, and client/server systems. The audit objective for determining the adequacy of using the service request system was eliminated during the course of the audit because the new Customer Relation Management System replaced this system.

INTRODUCTION

To determine the adequacy of the administration and management of the LAN/WAN, we reviewed the controls for the City network. Our testing and fieldwork consisted of obtaining and reviewing written policies, standards, and procedures in each area audited. Those areas included computer facilities, network design, and network administration. We also interviewed the administrators or managers to obtain an understanding of the functions performed by the LAN/WAN.

Overall Conclusion

If correctly implemented, the recent consolidation of the administration and management of the City LANs can have a positive impact on the efficiency and effectiveness of delivering City services while reducing the cost of City operations. However, much work is needed in defining and implementing standards for the operation and maintenance of the network infrastructure as well as the training and support requirements to position the City CIS staff to meet the new computing environment challenges.

The existing computing environment consists of multiple operating systems on workstations and networks. This environment poses significant challenges in providing adequate support for network operations and the workstations due to the complexity of simultaneously managing multiple operating systems on the networks. Training standards need to be defined for CIS personnel to operate and maintain the network. Departmental user training needs to be defined so that management can target training to meet the skill set requirements. Training should immediately follow development of the standards in those areas where the skills are not available by staff.

LAN/WAN policies and procedures in the areas of disaster recovery, change management, software inventory, software distribution, and software license verification should be defined and implemented to increase operational efficiencies, reduce the data security risks, and minimize legal liabilities to the City.

Physical and logical security continues to be a challenge. CIS has assessed the data and physical security needs, but adequate funding to implement many of these security needs is not currently available. Finally, environmental

INTRODUCTION

controls to safeguard sensitive equipment should be defined and implemented.

These and additional opportunities to improve the administration and management of the LAN/WAN are discussed in more detail in this report.

Background

The City has consolidated many of the information technology functions and processes from various departments under the direction and control of CIS. This consolidation created a requirement where the CIS staff must now address a myriad of support issues. CIS is now challenged with addressing diverse support issues as well as developing a set of homogeneous policies and procedures that will govern the administration and management of all departmental networks.

In accordance with the Control Objective for Information and Related Technology (COBIT), the audit guidelines for delivery and support include the following processes:

1. Manage performance and capacity to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs.
2. Manage problems and incidents to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence.
3. Manage data to ensure that data remains complete, accurate, and valid during its input, update, and storage.
4. Manage facilities to provide a suitable physical surrounding that protects the IT equipment and people against man-made and natural hazards.
5. Manage operations to ensure that important IT support functions are performed regularly and in an orderly fashion.

OPPORTUNITIES FOR IMPROVEMENT

We identified certain policies, procedures, and practices that could be improved. Our audit was not designed or intended to be a comprehensive study of the administration and management issues for each LAN, system, procedure, or transaction. Accordingly, the opportunities for improvement presented in this report reflect the level to which the analysis was focused.

1. Multiple operating systems pose significant challenges in providing adequate service, support, and network performance monitoring.

The City networks and workstations operate using several operating systems that pose significant challenges in the areas of service, support, network performance monitoring, and adequate workstation support. Although these systems are scheduled for conversion to a more limited set of operating systems in the next few years, CIS must ensure that it has adequately trained personnel to support the existing environment while implementing the new operating systems.

We found that the ability to effectively address operational support challenges that this environment presents are directly affected by multi-operating system support complexities, hardware and software standards, adequacy of training, and network management and monitoring capabilities.

A. Lack of strategy to implement hardware and software standards

Prior to the consolidation, each department developed and implemented different standards for network and workstation-computing environments. As a result of this decentralization, the City computing environment evolved into a wide array of hardware and software standards and operating systems. For example, the current workstation operating systems at the City include:

- Windows 95
- Windows 98
- Windows 2000
- Windows XP
- Linux
- IBM OS/2
- Apple MAC OS
- LINC

The network operating systems include:

- Windows NT
- Windows 2000
- Novell Netware
- UNIX
- Apple Network Operating System

To address the need for movement to a reduced set of hardware and software, CIS has developed hardware and software standards. These standards define the guidelines for all City departments to use when purchasing new hardware and software. These standards have been reviewed and approved by the Information Technology Executive Committee (ITEC). Compliance with the guidelines will

OPPORTUNITIES FOR IMPROVEMENT

improve the ability of CIS to support and maintain the equipment by minimizing the numerous types of systems needing support.

Standardizing on one or two network and workstation operating systems would certainly facilitate the management of the network. Discussions regarding movement to a reduced number of operating systems have occurred within CIS, but a formal strategy and implementation plan, including funding, has not been developed. Additionally, migration of legacy systems to newer operating platforms can reduce maintenance and support requirements.

B. Multiple operating systems highlight the need for a structured approach to training

In our interviews with Call Center and Desktop Support personnel, they indicated that they have the difficult and time-consuming task of troubleshooting issues that cause service disruptions. This support difficulty appears to be due to a lack of knowledge of problem remediation skills on each operating system and particularly Windows 2000. The stated goal of the Call Center (per a Service Improvements presentation dated 01/25/2002) is to “solve a customer’s problem on the first call whenever possible.” Having sufficient personnel to “solve a problem on the first call” in an environment supporting thirteen operating systems is a formidable challenge.

To remain abreast with all operating system issues as well as the issues of the different hardware platforms, highly focused training is needed for Call Center and Desktop Support personnel. Our review of training plans developed by CIS and Human Resources indicated that neither department has appropriate training materials for Call Center and Desktop Support personnel. CIS’ materials are inadequate, and Human Resources’ training materials are designed for end users.

CIS does not appear to have recently assessed its skill set requirements or developed a staff training plan for each employee. A common method used by CIS to develop a training plan is to derive the basic plan components from a gap analysis performed against a skill set matrix. The most current skill set matrix is dated October 2000. Since the consolidation of IT services, the types of support skills needed have increased. Additionally, employee turnover has made the October 2000 matrix outdated and inaccurate. Since the department does not possess a current skill set matrix, development of a training plan to support the stated goal of the Call Center will be difficult to achieve.

A solution to improve Call Center and Desktop support has been proposed by the Call Center manager. The solution is to consider outsourcing the Call Center support functions as a means of providing more consistent and accurate support. While outside firms may be able to address the support needs more effectively, it is unclear as to whether the cost is economically feasible. It should be noted that an outside firm would not be able to support the in-house developed LINC program.

OPPORTUNITIES FOR IMPROVEMENT

C. Installation of network management and monitoring tools is incomplete

The City uses BMC Patrol software to monitor key network devices such as hubs, switches, routers, and servers. BMC relies on software to be installed on the server and/or workstations to monitor and report operating conditions of equipment and software. Software for older network operating systems, such as Novell 4.11 and 5.x networks, was not originally available when the City purchased BMC Patrol. Subsequently, a software modification was made to allow monitoring of the Novell servers. In addition, our inquiry and review of the status of the Patrol software installation indicates that additional work is needed.

D. Internet “appropriate use” monitoring is sporadic

To monitor appropriate use of the Internet by City employees, the City obtained monitoring software called SuperScout. SuperScout limits and monitors Internet site usage. We tested the effectiveness of this software and found that inappropriate sites were accessible through the City’s Internet connections.

We recommend that CIS management:

A. Develop a strategy and plan to:

- Reduce the number of operating systems within the City.
- Develop a plan to ensure compliance with the hardware and software requirements adopted by ITEC.
- Migrate legacy systems to new platforms.

B. Improve the Call Center operations by:

- Identifying and developing the skill sets needed to support the CIS developed hardware/software standards.
- Ensuring adequate resources are available (personnel, software tools, etc.) to meet Call Center goals.
- Providing training to staff on City applications including InfoAdvantage, the Citizen Request Management System, CAPS, etc.
- Considering outsourcing technical support.
- Reducing calls to the center by co-developing with Human Resources a training curricula and plan based upon CIS hardware/software standards.

C. Complete the installation of the BMC Patrol software to all City network devices to enable these networks to be centrally monitored by CIS.

D. Ensure that the software (SuperScout) monitoring access to Internet sites is operating and in accordance with interim Administrative Directive (AD) 2-33 at all times.

OPPORTUNITIES FOR IMPROVEMENT

Management's Response:

- A. • CIS agrees with the recommendation to reduce the number of operating systems within the City. The citywide software standard was developed in 2001, which established the workstation and server operating system standards. The workstation software standard is currently Windows 2000. Existing Windows 98 and Windows NT 4.0 workstations will be grandfathered until the units can be replaced. The server software standard is Microsoft 2000 Server and Microsoft 2000 Advanced Server. In March of 2001, CIS contracted with Dell and Xerox Connect to lease and purchase PC's and servers with this standard. The contract ensures that the operating system software standards would be implemented on newly leased and purchased PC's and servers.

In September of 2001, citywide Server Management became the responsibility of the CIS Department. CIS conducted server assessments to determine the scope of work and funding required to establish the server operating system standard on existing servers. Implementation of the standard will be completed according to plans, pending funding approval.

- CIS agrees that LINC legacy systems should be migrated to new platforms. In 1999 CIS developed a Strategic Plan that identified the movement of all applications from LINC. This plan will be updated yearly to migrate legacy LINC systems to new platforms. It is estimated that it will take three years or more to completely migrate all systems from LINC, based upon funding to replace existing systems (i.e., replace Computer Aided Dispatch for estimated \$20 Million).
- B. • Call Center skill sets have been identified based on industry standards. Based on these standards, the Call Center staff should be trained to be Microsoft Certified Systems Engineers, along with extensive networking and software product knowledge. Tuition and testing certification for 7 FTE's is estimated at \$64K with a two-year completion goal. Software and product expertise training is estimated at \$14K, network knowledge training is an additional \$7K, and customer service skills training \$3.5K. Although the Call Center skill sets have been identified, restricted training budgets have not allowed these expenditures.

CIS is also considering outsourcing the Call Center. On January 28, 2002, the CIO presented his business case to the City Council's Privatization Committee on the outsourcing of the help desk functions. A RFCSP (BUZ0220) Enterprise Help Desk Services has been advertised and is to be opened on April 02, 2002.

- CIS will request adequate resources to meet Call Center goals as necessary, pending the outcome of the Help Desk outsourcing efforts.

OPPORTUNITIES FOR IMPROVEMENT

- CIS agrees that training on City applications is important and staff should have a good understanding of application's functionality. We do not expect staff to be experts in every application. A subject specialist who works with a particular application on a daily basis should provide advanced support and expertise of the application at the departmental level.
 - On January 28, 2002, the CIO presented his business case to the City Council's Privatization Committee on the outsourcing of the help desk functions. A RFCSP (BUZ0220) Enterprise Help Desk Services has been advertised and is to be opened on April 02, 2002.
 - CIS agrees that a training curricula and plan based upon CIS hardware and software standards is needed. Citywide training is a function of the Employee Development/Training Division of Human Resources.
- C. CIS agrees with this finding, with one minor clarification. BMC Patrol software can only be installed on servers. Other network devices can interface with the Patrol Enterprise Manager (PEM), using different software. A server installation plan for BMC Patrol has been developed for City Hall, OCMC, and Old City Hall Servers. The schedule for other suitable servers will be developed later this fiscal year. All servers do not meet the minimal requirements for BMC Patrol software installation. BMC Patrol will not be installed on these servers, which will gradually be phased out or replaced.
- In order to retrofit other existing network devices to interface with the PEM, additional funding will be required. This project will be completed at the end of FY 03-04 pending funding approval.
- CIS will also develop a boiler plate insert that will be added to all RFCSP's to insure that BMC Patrol agents and other network device software are included as part of the specifications for new servers and other network devices. This insert will also include other security, database, and network requirements.
- D. AD 2-33 received final approval on 3/01/02. CIS agrees that Internet site monitoring is needed and that it should be in operation in accordance with AD 2-33 at all times. In conjunction with the rollout of the new network, CIS will continue to employ SuperScout to achieve the goals of the Administrative Directive.

OPPORTUNITIES FOR IMPROVEMENT

2. LAN/WAN operational policies and procedures have not been fully defined and implemented.

Our audit identified policies and procedures that are incomplete in numerous operational areas. The areas reviewed include disaster recovery and business continuity, financial due diligence reviews, change management, hardware/software inventory, software licensing and distribution, logon procedures, and equipment configuration.

A. Failure to implement a Disaster Recovery/Business Continuity Plan places the City at risk

The City has not implemented the Disaster Recovery/Business Continuity Plan approved in May of 2001. In May of 2001, the City Council approved a contract to engage the firm of Comdisco to provide backup and recovery facilities. Upon review of the financial health of the firm by the City Auditor's Office, we recommended to CIS that the City not contract with this firm and seek another firm to provide those services. Comdisco declared bankruptcy a few weeks later. As of December 2001, an alternate firm has not been selected and engaged to act as our recovery service. We believe the lack of a hot-site backup places the City at risk should a catastrophic event occur.

Additional areas of concern regarding disaster recovery include:

- Standard backup and recovery procedures and policies are still in draft form.
- Standards for off-site secure storage and tape rotation are in draft form.
- Standards for periodic testing of data recovery are in draft form.

A Disaster Recovery/Business Continuity Plan sets the standards for off-site secure storage, backup and recovery policies, system redundancy, backup power (UPS), and the maintenance of documentation that relates to LAN facilities. The goal is for the Disaster Recovery/Business Continuity Plan to define the structure needed for the City to recover as quickly as possible from any operational crisis.

B. Failure to perform financial due-diligence places the City at risk

A review of the financial status of Comdisco was not undertaken as required by the CIS Procedures Matrix Project Checklist, item 36. Although the checklist only specifies that a credit report be obtained on the prospective contractor, CIS did not obtain the report. Comdisco was in extreme financial difficulty when the City Council approved the contract for disaster recovery (May 2001). Comdisco filed for bankruptcy under Chapter 11 on July 16, 2001. The City should thoroughly review a vendor's financial status before the City considers a contract with that vendor.

OPPORTUNITIES FOR IMPROVEMENT

C. The change management procedure has not been approved

A formal AD covering Change Management is not in effect. CIS Quality Assurance personnel have been working on a draft AD since June 2000. The current draft (AD 2-28) defines the Citywide Change Management Plan. Failure to implement the policy may cause procedural confusion within the departments when requesting a system change. This policy should become operational as soon as possible as it defines the control mechanisms required of end-users and CIS to effect changes to production systems in a uniform and structured manner.

The draft AD has been distributed to departments for comment and training on change procedures has been offered to departments and users that are directly involved in initiating the change or addition.

D. CIS does not maintain an inventory system to manage network devices and software

A system to identify hardware and software operating on the City networks is not in place. Although CIS has a listing of hardware and software for the mainframe, an inventory system that tracks workstations, installed software, network devices, and IP addresses does not exist. An automated or a manual system is necessary for support personnel to:

- Be aware of equipment and software configurations when they are providing problem resolution from the CIS Call Center.
- Monitor software license compliance.
- Readily identify workstation configuration while providing support.

E. Lack of software licensing monitoring capabilities places the City at legal risk

A system to monitor software license compliance for the City is not currently implemented. This lack of monitoring could result in penalties, fines, and lawsuits due to software licensing violations. To address this issue, the City needs to implement a system to inventory and assess the software currently installed on the network. The results would provide network managers with appropriate information to remove unauthorized software on City networks or procure additional licenses for that software.

F. Automated software distribution can provide quick reaction time to security threats and improve desktop support efficiency

CIS does not have an automated software distribution capability for the City's network environment. Software is installed and updated manually by Desktop Support technicians. As a result of the manual efforts needed to install software, the City is impeded from efficiently installing software and software updates, which protect the City from current security threats. On many occasions, operating system software updates are needed to resolve processing and security issues, and their timely distribution is critical. This capability would reduce or eliminate the need for

OPPORTUNITIES FOR IMPROVEMENT

CIS service technicians to have to go to each workstation to distribute new software, patches, upgrades, and security software.

The ability to perform software distribution centrally would also allow network managers to update workstations with the most current software security updates. When software security threats are announced and updates released, CIS needs the capability to immediately distribute the updates to all City workstations. This capability will reduce the threat of viruses or other security threats from spreading throughout the network.

G. Lack of single sign-on capability jeopardizes system security and productivity

The City does not have the capability to provide a single sign-on for users. This capability is provided through the use of software that authorizes access to different systems on the network. City employees are now required to login to several application systems before they begin their work. End-users have to log on an average of four systems (i.e., Novell, Lotus Agenda System, Windows, GroupWise, CMO LAN, and Controller Resource) to access system resources. Each login activity can take several minutes to complete and end-users must also remember four user ID and password combinations. Users sometimes address this difficulty by writing the various login/password combinations on a piece of paper, which they keep at their desks. Written login/password combinations can create a security vulnerability. On the other hand, when employees forget their ID/password combination, they call the Call Center to request password resets, which increases Call Center activity.

H. The ability to quickly restore network devices after failure may be affected by the lack of documented procedures

Specific procedures to re-configure a network device after failure do not exist. Trained CIS personnel rely on the equipment's operation manual (when available) and a printout of the equipment configuration to restore failed equipment. To ensure rapid restoration of service, a detailed procedure for bringing equipment back on-line should be developed and included in the Disaster Recovery/Business Continuity Plan. These procedures should include specific and/or unique steps and situations that could deviate from the manufacturer's installation specification. These situations may include software installed, service packs used, operating system services enabled or disabled, fixed or dynamic routing paths, and switch settings.

We recommend that the CIS management:

- A. Finalize and implement the disaster recovery plan by:
- Defining all backup policies and procedures.
 - Defining the standards for off-site storage of backup media.

OPPORTUNITIES FOR IMPROVEMENT

- Developing a plan that defines a timetable for periodic testing of data recovery.
 - Finalizing contract with vendor.
- B. Perform a comprehensive financial review of all prospective contractors.
- C. Finalize and implement the new Citywide Change Management Administrative Directive – AD 2-28.
- D. Implement a hardware and software inventory tracking system on all connected devices. Devices not connected need to be defined.
- E. Procure software able to monitor software-licensing compliance and perform on-going compliance review.
- F. Identify and implement the process necessary to distribute software from one central point and enforce uniformity of software across all departments.
- G. If cost beneficial, procure software that would allow a single sign-on for operational systems.
- H. Require written detailed documentation, in addition to the original equipment configuration specification and manual, that explains how to restore the operational configuration of network devices. The required documentation would explain the steps needed to restore the operational configuration of hubs, switches, firewalls, and other network appliances. This documentation should be stored on-site in close proximity to the equipment.

Management's Response:

- A. • CIS agrees that backup policies and procedures should be redefined. The backup policies and procedures are included in AD 2-34, Data Backup and Recovery Policy Standard and Procedures for the Mainframe and Server. The process to approve this AD will begin in April 2002 and will be completed by September 2002.
- CIS agrees with this recommendation and has already developed standards for off-site storage of backup media. The standards for off-site storage of backup media are included in AD 2-34, Data Backup and Recovery Policy Standard and Procedures for the Mainframe and Server. The process to approve this AD will begin in April 2002 and will be completed by September 2002.

OPPORTUNITIES FOR IMPROVEMENT

- This item has been addressed. A plan outline has been created that defines a timetable for periodic testing of data recovery. The outline is included as part of AD 2-29, which will be released for department comments in April 2002.
 - This item has been addressed. The contract for a Disaster Recovery Hot Site with SunGard was approved on 2/20/02.
- B. The City needs to designate a department to perform comprehensive financial reviews of all prospective contractors. Until a department has been designated to perform this function, CIS will employ the services of the City Auditor's office to assist with financial reviews of CIS prospective contractors.
- C. This item has been addressed. AD 2-28 received final approval on 2/20/02, and became effective on 3/01/02.
- D. CIS concurs with the audit finding. In FY2000-2001, an RFCSP was released for the procurement of an asset management system but was cancelled due to the transfer of responsibilities for leased and purchased computers from CIS to the respective departments. This transfer was initiated by the Purchasing Department and resulted in a loss of asset management personnel and funding to procure the system.
- E. CIS concurs with the audit finding. Additional funding will be required to adequately monitor software-licensing compliance, and to perform ongoing compliance reviews. CIS will develop a BAF in FY 03-04 to acquire and implement this recommendation upon completion of the implementation of Exchange.

Several steps have already been taken to establish Enterprise-wide license agreements for standard software. Enterprise-wide agreements have been established with Novell, Microsoft, ESRI, Oracle, and Symantec for standard software products. Licensing for the software products covered under these agreements ensure software license compliance.

- F. CIS concurs with the audit finding. Various software distribution products were reviewed and rejected by CIS staff, due to the diverse server operating systems within the City. Many of the initial roadblocks to a software distribution system were removed with the establishment of the Windows 2000 Server operating system standard approved by ITEC.

A committee will be established to study the software distribution issue and identify the best software distribution product available. This committee will identify the true cost of procurement, deployment, security, management, and maintenance of a software distribution system. The committee will be established in May 2002. Product review and analysis will take place in May, June, and July of 2002. If approved by the CIO, ITEC, and by the budget process, the software distribution software will be acquired and implemented within the 2003-2004 fiscal year.

OPPORTUNITIES FOR IMPROVEMENT

- G. CIS has reviewed several different software applications for Single-Sign-On (SSO) capability including IBM, CA and BMC. At this time, it does not appear to be cost-effective to implement SSO because of the disparate systems and internally written LINC operating system currently deployed throughout the city. As application within these operating systems are replaced, CIS has been aligning them with our current NT infrastructure, allowing CIS to use a single NT user account and password for access to multiple applications.
- H. CIS agrees that written detailed documentation should be available for all network devices, however the information should be stored both on-site and off-site (in the event of a disaster). Network Engineering has installed, along with the new data infrastructure, Cisco Works 2000 and modules to download configuration data of routers, switches and other networking devices to a central site on a daily basis for quick referral. Along with this the current configuration, the current IOS for each type of switch and router is also saved to the TFTP services offered under Cisco Works 2000

In the event of a failure, the replacement box will be configured to receive all of its operational software and the current configuration from the TFTP Service. The Cisco Works database will be backed up according to current procedures with copies kept in off-site disaster storage. A configuration procedure will be developed to instruct engineers in the initial configuration in order to receive the download from Cisco Works 2000.

3. Physical and logical data security issues are not resolved.

Data security concerns remain and are being affected by funding issues. The City Auditor performed a review of the security of data and telecommunication equipment for the period July 17, 2000, to August 31, 2000. One finding identified that physical security risks existed for key network components. This issue continues to remain.

A. Physical Security

- Doors to sensitive network equipment continue to be unsecured during normal business hours in City Hall. This condition provides any visitor to City Hall the opportunity to harm equipment vital to the operation of the network infrastructure.
- Inventory storage areas are not centralized and secured. For example, equipment such as monitors, computers, and keyboards are stored in the passageway from the Wellness Center to the parking garage and in the passageway connecting City Hall to the Convention Center on L2.
- Sensitive equipment has limited protection from dust, fire, smoke, and food.

OPPORTUNITIES FOR IMPROVEMENT

Other issues affecting security include:

B. Funding for identified security needs

Although a long-range plan to enhance security has been defined, funding has not been identified and committed to implement the plan. CIS has identified security needs in a proposed departmental long-range plan. CIS should continue to enhance security efforts with the goal of implementing their identified requirements in the upcoming fiscal year(s). The CIO should have provided the City Manager with a plan of the funding requirements to implement the security needs.

Data security risks

A review of the data security systems currently in place indicate that security breaches may originate from uneven monitoring, lack of adequate security software, lack of virus software and updates to that software, and inadequate user training on data security. Lack of attention in these areas has resulted in the following conditions:

C. Security Policy

- CIS security policy on the Intranet is outdated.
- Policies and procedures that define the security for access to computing facilities are not in place. For example, when an individual enters the server area, they are able to access all of the equipment in that area even if they are not authorized to do so.

D. Access Security

- A policy to maintain access logs to secured areas does not exist.
- A security violations response team and reporting system does not exist.

E. Lack of effective network monitoring. Areas needing improvement include identification of the source and nature of the security violation, limiting intruder damage, and maintenance of forensic data for security incidents.

F. Installation of standard anti-virus protection software on all City network devices and workstations is incomplete.

G. Employees do not consistently lock their workstations when leaving their work area, allowing other users unauthorized access. Windows 2000 provides a mechanism to prevent access to a computer, but other operating systems such as Windows 95/98 do not provide this security.

H. CIS Security is not consistently involved in system development planning efforts. Therefore, CIS must try to address security needs after funding for the projects has been approved.

OPPORTUNITIES FOR IMPROVEMENT

We recommend that CIS Management:

- A. Resolve physical security issues identified in this and the previous audit report. (Secure all doors to sensitive network equipment and inventory storage. City staff should monitor vendors' access rights and ensure the areas are secured when vendors have completed their work.)
- B. Develop a formal long-range security plan and include funding requirements in each of the annual City budgets to implement the recommended security measures.
- C. Develop a policy and procedure that defines the access and logging requirements into CIS secure areas. This policy should include a list of people who are accessing or who have permission to access the CIS main server room.
- D. Develop and implement a data security policy. This policy should contain:
 - o A definition of levels of access to the LAN by administrators and users.
 - o Process for keeping and reviewing a log of access violations.
 - o Policies that will be implemented if access violations occur.
- E. Consider purchasing forensic software and training for monitoring security violations on client/server and other distributed systems.
- F. Implement a Citywide virus protection program immediately.
- G. On-going training should be provided to users regarding implementing security on their individual workstations and on the LAN.
- H. Require development projects to coordinate with CIS Security during the project initiation phase

Management's Response:

- A. CIS concurs that all doors to sensitive network equipment should be secured. As tenants within a building our function is not to secure doors. CIS will request additional security measures be implemented to comply with the audit findings, however this recommendation should be addressed by Building Management/Building Security. It is understood that not all vendors within City Hall are CIS vendors, however CIS vendor access to CIS areas are monitored thru the security badge system.
- B. CIS concurs with the audit finding. A business case was developed in 2000 with the City Auditor to implement recommendations of the security assessment. CIS is requesting additional funding in FY 02-03 to implement Phase II of the plan.

OPPORTUNITIES FOR IMPROVEMENT

- C. CIS agrees with this recommendation. A business case has been developed in order to implement the security assessment. CIS is requesting additional funding to implement Phase II of the plan, which will include access and logging requirements.
- D. CIS agrees with the recommendation and has begun the framework for an Enterprise Security Policy. CIS knows that this policy is the most important facet of any enterprise security plan. CIS has targeted the end of this calendar year to complete the policy.
- E. CIS concurs with the audit finding. Training for CIS staff will be provided with the acquisition of this software. This will be accomplished when training and travel budgets are reinstated.
- F. CIS concurs with the audit finding. Rollout of the citywide virus protection program began in October of 2001, and is currently 85% complete. The project will be 100% complete by the end of this calendar year.
- G. CIS concurs that training should be provided to users of the system, however CIS is currently not staffed or equipped to provide citywide user training. Over the years, both training budgets and training personnel within CIS have been consistently removed from the CIS budget. The Employee Development/Training Division of Human Resources would be better suited to undertake a citywide training program for users. CIS will work closely with Human Resources to assist in every way possible to ensure that they have the information needed to provide this training.
- H. CIS concurs with the audit finding. Development projects are required to coordinate with CIS Security during the Initiation Phase as well as the other project phases. A security section will be added to all future technology acquisition requests, to ensure compliance with all security requirements and regulations.

This report is intended to promote the best possible management of public resources. You are welcome to keep this copy if it is useful to you. If you no longer need the report, you are encouraged to return it to:

Office of the City Auditor
City of Dallas
1500 Marilla, Suite 2FN
Dallas, TX 75201

We maintain an inventory of past audit reports and your cooperation will help us save on copying costs.