Chapter III - Reviewing Personal Computers and Local Area Networks

Introduction

More and more applications are running on personal computers (PC) and local area networks (LAN) everyday. The reasons for the migration of applications from mainframes to PCs are simple: ease of use, speed and cost.

Some applications run entirely on PCs. These are generally small applications where one user is responsible for the system. For example, a small agency with a small accounts receivable system might run the system on a PC on the user's desk.

Other applications run partly on PCs and partly on other computers called servers. Generally speaking, these systems are called client/server systems. These systems take advantage of the PC's ease of use and the processing power of larger computers. The server computers range from powerful PCs to minicomputers to mainframes.

Networks link the different computers together, and when all of the computers are in the same office, the network is called a local area network. LANs permit PCs to communicate with each other and share common resources such as printers. LANs support office automation applications like electronic mail and on-line appointment calendars, and permit users to easily transfer documents among themselves.

When one of the computers on the LAN is a communications server or gateway device, the PCs on the LAN can connect with other LANs and computers in remote locations. Connections with mainframe computers permit PCs to work like mainframe terminals, giving the users access to mainframe application systems.

This chapter presents audit objectives, possible controls, suggested audit procedures and comments on reporting findings for the auditor to use when reviewing an application system that runs at least in part on PCs or LANs. The auditor should use this material to supplement Chapter II, Reviewing Application Systems, whenever a significant application system runs on PCs.
Section 1. Personal Computers and Local Area Networks

Management should understand that the use of personal computers for financial applications is risky because controls present on larger computers may be missing. For example, there may be no program change controls, user access restrictions, or data backup procedures. The risks associated with using personal computers for financial applications should be fully understood by management.

Access to sensitive data files and critical applications should be restricted according to job duties. It is easier to secure files stored on a LAN file server than on a standalone or workstation personal computer. The security should include personal identification with individual logons and confidential passwords. Also, the security should restrict the ability of individuals to read or change sensitive data files, and perform specific application functions.

Whenever data is transferred from one computer to another, there is a risk of data corruption or loss. Whenever programs are transferred, there is a risk of virus infection. To protect against data loss, error detection routines during transmission and control totals should be used. To protect against virus infection, new programs should be scanned for the presence of viruses before being loaded to agency computers, and hard disks should be scanned periodically.

Systems should be developed and maintained according to user specifications. Custom made software should be developed according to appropriate standards. Programmers, either internal or external, should comply with the agency's systems development methodology. End users, who sometimes build their own systems, should comply with the agency's end user computing standards. Both of these standards should establish minimum requirements for system testing and documentation.

Vendor supplied software, both operating systems and application systems, should be managed in an orderly way. Installation should be done according to instructions, upgrades should be tested and installed uniformly for all related personal computers. Detailed records of hardware configurations and software versions should be kept to ensure maintainability and compliance with licensing restrictions and copyright laws.

Financial application users should have appropriate documentation and training to make sure that the system is operated as planned.

Data and program files should be regularly backed up and stored offsite. The frequency of the backups should correspond with the number and frequency of changes to the files. Several generations of backups should be stored in a secure, environmentally protected remote location. Copies of the documentation should also be stored offsite to ensure the recoverability of the system.
Audit Objectives

The auditor should determine whether personal computers and local area networks, when used for financial applications, adequately support the reliable operation of the applications.

Possible Controls

1. When personal computers or local area networks are used for financial applications, the agency may have a policy about end user production computing that addresses one or more of the following:
   (A) Management authorization of PCs or LANs for production application systems, whether financial or otherwise.
   (B) Protection of data files on PCs or file servers from unauthorized access.
   (C) User responsibility for data integrity during storage and transmission.
   (D) Standards for the development of PC or LAN based systems including program change controls and documentation requirements.
   (E) Backup requirements for data and programs so that the system is recoverable in case of disaster.
   (F) End users who download data for management analysis and decision-making are responsible for the completeness, accuracy and security of the data.

2. When personal computers are used for processing, the agency may use one or more of the following controls to ensure that sensitive data files stored on personal computers are protected.
   (A) Files stored on a file server are protected by LAN security software so that persons are identified and access to files is suitably restricted.
   (B) Personal computers, which store sensitive files, are kept in a restricted area and locked after hours.
   (C) Sensitive data is stored in encrypted form, and only authorized users can decrypt it.
   (D) Personal computer keyboard or on/off switch is locked, and only authorized users have keys.
3. When personal computers are used for processing, the agency may use one or more of the following controls to ensure that programs stored on personal computers are protected.

   (A) Users have access to the executable programs (object code) only, not the programmer's versions (source code).

   (B) Users have access to the source code, but these programs are verified for integrity each time they are run.

4. When developing systems to operate on PCs or LANs, the agency may use one or more of the following controls:

   (A) PC and LAN application systems are developed and maintained by the systems development staff according to the same standards used for mainframe software.

   (B) PC and LAN application systems are developed and maintained by departmental staff or end users according to standards that require:

       (1) Written user specifications.
       (2) Testing of changes before installation.
       (3) Documentation of changes, including both system and user documentation.
       (4) User acceptance of changes before implementation.

5. The agency may use one or more of the following controls to ensure the correct use of purchased software (operating systems and applications).

   (A) Each upgrade is tested and approved by management before distribution to users.

   (B) When upgrading software, the previous version of the software is retained in case problems arise with the upgraded version.

   (C) The agency maintains an inventory of software versions which is current and correct. The inventory is adequate to identify any uninstalled upgrades, and ensure compliance with licensing or copyright restrictions.

   (D) Users receive adequate training and instruction manuals for the operation of the purchased application system.
6. When the agency operates PC or LAN based production application systems, there are controls to prevent the loss or alteration of data during transmission to or from other computers:

(A) Transmission hardware or software contains error checking routines to make sure the data is not changed during transmission.

(B) Diskettes used to transfer data between computers are clearly and correctly labeled.

(C) Control totals are used to make sure that no items, batches or groups of batches are lost during the exchange.

7. The agency may use one or more of the following controls to protect against computer viruses:

(A) Personnel are prohibited from copying personal software onto agency personal computers.

(B) Incoming diskettes are checked for viruses before being copied onto agency personal computers.

(C) Hard disks are periodically scanned for the presence of known viruses.

8. The agency protects against data loss and ensures the recoverability of the system through one or more of the following controls:

(A) Users maintain original source documents for a period of time if needed for re-input.

(B) Users back up data files daily or weekly.

(C) Systems maintenance staff back up program files whenever they change.

(D) Backup data and program files are properly labeled and rotated to a secure offsite location where several generations of backup are kept. The offsite location is safe from damage by heat, humidity, magnetic fields and static electricity.

(E) Documentation is also stored in the secure offsite location.
Suggested Audit Procedures

1.1 Inquire of management about its use of personal computers for critical applications or sensitive information. Examine policy statements to see if they address all the risks, including security, data integrity, development standards, and backup.

1.2 Examine the security system and verify that sensitive data files and critical programs are protected against unauthorized use or change.

1.3 Inquire as to how agency applications are developed and maintained. Examine the documentation to make sure that changes are requested in writing, tested, documented and accepted by users before being put into production.

1.4 Observe the agency's practices concerning the installation of purchased software. Make sure that upgrades are tested, and versions are controlled through an inventory of installed software.

1.5 Inquire about the means that the agency uses to ensure completeness when data is transferred to other systems either via communications links or by diskette exchange.

1.6 Examine the procedures used by the agency to prevent virus infections.

1.7 Examine the data backup procedures and verify that the application system is recoverable in case the original data files are lost or destroyed.

Comments on Reporting Findings

These controls and audit procedures should not be applied to all personal computers and local area networks, only those that are used to run significant application systems. However, when significant applications run on PCs and LANs, these controls should be in place.