EXPOSURE DRAFT ISSUED FOR CONSULTATION UNTIL 5 SEPTEMBER 2003

Annex II

PRACTICE NOTE

1001

IT ENVIRONMENTS – STAND-ALONE PERSONAL COMPUTERS

(Issued [ ] 2003)

The purpose of Practice Notes issued by the Hong Kong Society of Accountants is to assist auditors in applying Statements of Auditing Standards (SASs) and Standards on Assurance Engagements (SAEs) of general application to particular circumstances and industries.

They are persuasive rather than prescriptive. However they are indicative of good practice and have similar status to the explanatory material in SASs and SAEs, even though they may be developed without the full process of consultation and exposure used for SASs and SAEs. Auditors should be prepared to explain departures when called upon to do so.

Introduction

1. This Practice Note (PN) describes the effects of stand-alone PCs on the accounting system and related internal controls and on audit procedures.

Stand-Alone PCs

2. PCs can be used to process accounting transactions and produce reports that are essential to the preparation of financial statements. The PC may constitute the entire computer-based accounting system or merely a part of it.

3. Generally, information technology (IT) environments in which stand-alone PCs are used are somewhat different from other IT environments. Certain controls and security measures that are used for large computer systems may not be practicable for PCs. In contrast, certain types of internal controls become more important because of the characteristics of stand-alone PCs and the environments in which they are used.

4. Stand-alone PCs can be operated by a single user or many users at different times accessing the same or different programs on the same computer. The user of a stand-alone PC that processes accounting applications performs many functions (for example, entering data and operating application programs). While typically not knowledgeable about programming, users may often use third-party or off-the-shelf software packages such as electronic spreadsheets or database applications.

5. The organizational structure within which a stand-alone PC is used is important in assessing risks and the extent of the controls required to mitigate those risks. For example monitoring controls employed by management may be the only effective controls for a purchased software package used by a small business on a stand-alone PC apart from whatever controls are incorporated in the package itself. In contrast, the effectiveness of controls relating to a stand-alone PC used within a larger organization may depend on an organizational structure that clearly segregates responsibilities and restricts the use of the stand-alone PC to specific functions.

6. The control considerations and the characteristics of the hardware and software are different when a PC is linked to other computers. Such situations often lead to increased risks. This PN does not address the auditors' consideration of network security and controls. This PN is however relevant for PCs that are linked to another computer, but can also be used as stand-alone workstations. Many PCs may be used interchangeably as part of a network or in stand-alone mode. When dealing with such PCs, the auditors consider the additional risks encountered by access through a network as well as the guidance in this PN.

Internal Control in Stand-Alone PC Environments

7. PCs are oriented to individual end-users. The degree of accuracy and reliability of financial information they produce will depend, in part, on the internal controls that the user adopts either voluntarily or because management has prescribed them. The control procedures implemented relate to the complexity of the business environment in which the PC operates. Ordinarily, the stand-alone PC environment is less structured than a centrally controlled IT environment. In the former, users with only basic data processing skills can implement application programs relatively quickly, triggering issues such as the adequacy of systems' documentation or access control procedures. Such users may not regard controls over the application implementation process (for example, adequate documentation) and operations (for example, access control procedures) as important or cost-effective. In such circumstances, because the financial information is processed on a computer, users may tend to place unwarranted reliance on it.

8. In a typical stand-alone PC environment, the level of general controls is lower than what would be found in a large-scale computing environment. Nevertheless, selected security and control procedures can help improve the overall level of internal control.

Organizational Policies and Procedures

9. As part of the acquisition of an understanding of the control environment, and hence the IT environment for stand-alone PCs, the auditors consider the organizational structure of the entity and, in particular, the allocation of responsibilities for data processing. Effective policies and procedures for the acquisition, implementation, operation and maintenance of stand-alone PCs can enhance the overall control environment. A failure to implement such policies may lead to the entity using out of date programs and to errors in the data and the information derived from them, and may lead to an increased risk of fraud. Such policies and procedures include the following:

   a. acquisition, implementation and documentation standards;

   b. user training;

   c. security, back-up and storage guidelines;

   d. password management;

   e. personal usage policies;

   f. software acquisition and usage standards;

   g. data protection standards;

   h. program maintenance and technical support;

   i. an appropriate level of segregation of duties and responsibilities; and

j. virus protection.

Physical Protection—Equipment

10. Because of their physical characteristics, stand-alone PCs and their storage media are susceptible to theft, physical damage, unauthorized access or misuse. They can be physically protected by:

a. locking them in a protective room, cabinet or shell;

b. using an alarm system that is activated if the PC is disconnected or moved from its location;

c. fastening the PC to a table;

d. policies outlining the proper procedures to follow when traveling with a laptop or using it off premises;

e. encryption of key files;

f. installing a locking mechanism to control access to the on/off switch. This may not prevent PC theft, but may be effective in controlling unauthorized use; and

g. implementing environmental controls to prevent damages from natural disasters, such as fire, floods, etc.

Physical Protection—Removable and Non-Removable Media

11. PC programs and data can be stored on removable or non-removable storage media. For example, diskettes and CDs can be removed physically from the stand-alone PC, while hard disks are normally contained in the PC or in a stand-alone unit attached to it. In addition, the interior components (including the hard drive) of many PCs, in particular laptops, are easily accessible. When many individuals use a particular PC, storage media are more likely to be misplaced, altered without authorization or destroyed.

12. It is the user's responsibility to protect removable storage media by, for example, keeping current backups of such media in a fireproof container, either on site, off site, or both. This applies equally to operating systems, application programs and data.

Program and Data Security

13. When PCs are accessible to many users, there is a risk that the operating system, programs and data may be altered without authorization, or that users may install their own versions of programs giving rise to potential software licensing liabilities.

14. The degree of control and security features present in a PC operating system vary. Although some operating systems contain sophisticated built-in security features, those used on stand-alone PCs generally do not. Nevertheless, there are techniques to help ensure data are processed and read as authorized and that accidental destruction of data is minimized. The following techniques can limit access to programs and data to authorized personnel:

a. using passwords;

b. implementing an access control package;

c. using of removable storage media;

d. using hidden directories and files; and

e. using encryption.

15. An effective control technique is to use profiles and passwords, which control the level of access granted to a user. For example, a user may be given a profile protected by a password that allows data entry only, and a stand-alone PC might be configured to require a password before it can be "booted-up."

16. In some instances an access control package can provide effective control over the access to and use of operating systems, programs and data. For example, only a specific user may have access to the password file or be allowed to install programs. Such packages can also regularly examine programs on the PC to detect whether unauthorized programs or versions of programs are being used.

17. The use of removable storage media for critical and sensitive programs and data can provide enhanced protection by being kept off-line and under independent control until required. For example, salary data in a payroll system may be kept off-line and used only when required for payroll processing.

18. Removing programs and data from PCs with removable storage media (for example, diskettes, CDs and cartridges) is one effective way to keep them secure. The media are then placed in the custody of the file librarians or the users responsible for the data or programs.

19. Encryption is a technique that is generally used when sensitive data are transmitted over communication lines, but it can also be used on data stored on a stand-alone PC.

Continuity of Operations

20. In a PC environment, management typically relies on the user to ensure the continued availability of the systems in the event of a failure, loss or destruction of the equipment, operating system, programs or data. This will entail:

a. the user retaining copies of the operating systems, programs and data, with at least one copy stored at a secure location away from the PC; and

b. access being available to alternative equipment within a reasonable time given the use and importance of the underlying system.

The Effect of Stand-Alone PCs on the Accounting System and Related Internal Controls

21. The effect of PCs on the accounting system and the associated risks will generally depend on:

a. the extent to which the PC is being used to process accounting applications;

b. the type and significance of financial transactions being processed; and

c. the nature of programs and data used in the applications.

22. Below is a summary of some of the key considerations and their effects on both general and application controls.

General Controls—Segregation of Duties

23. In a PC environment, users can generally perform two or more of the following functions in the accounting system:

a. initiating source documents;

b. authorizing source documents;

c. entering data into the system;

d. processing data that have been entered;

e. changing programs and data;

f. using or distributing output; and

g. modifying the operating systems.

24. In other IT environments, such functions would generally be segregated through appropriate general controls. This lack of segregation of functions in a PC environment may allow errors to go undetected and permit the perpetration and concealment of fraud.

Application Controls

25. The existence and use of appropriate access controls over programs and data, combined with controls over input, processing and output of data may, in coordination with management policies, compensate for some of the weaknesses in general controls in PC environments. Effective controls include the following:

a. programmed control procedures, such as limit checks;

b. a system of transaction logs and batch balancing, including follow up and resolution of any exceptions;

c. direct supervision, for example, a review of reports; and

d. a reconciliation of record counts or hash totals.

26. Control may be established by an independent function that generally:

a. receives all data for processing;

b. ensures that all data are authorized and recorded;

c. follows up all errors detected during processing;

d. verifies the proper distribution of output; and

e. restricts physical access to application programs and data.

Separate controls are ordinarily required over master file and transaction data.

The Effect of a Stand-Alone PC Environment on Audit Procedures

27. In a stand-alone PC environment, it may not be practicable or cost-effective for management to implement sufficient controls to reduce the risks of undetected errors to a minimum level. In this situation, after obtaining the understanding of the accounting system and control environment required by SAS 300 “Audit risk assessments and accounting and internal control systems”, the auditors may find it more cost-effective not to make a further review of general controls or application controls, but to concentrate audit efforts on substantive

procedures. This may entail more extensive physical examination and confirmation of assets, more tests of transactions, larger sample sizes and greater use of computer-assisted audit techniques (see PN 1009 "Computer-assisted audit techniques").

28. Where the level of general controls appears adequate, the auditors may decide to adopt a different approach. For example, an entity processing a large number of sales transactions on a stand-alone PC may establish control procedures that reduce control risk.

29. Stand-alone PCs are frequently encountered in small entities. [PN 1005 "The special considerations in the audit of small entities"] provides further guidance. Based on a preliminary review of controls, the audit plan might include testing the controls the auditors intend to rely on.

Compatibility with International Auditing Practice Statements

30. This Practice Note is, in all material respects, in accordance with International Auditing Practice Statement 1001 "IT Environments – Stand-Alone Personal Computers".