# PRACTICE NOTE

# 1002

# IT ENVIRONMENTS – ON-LINE COMPUTER SYSTEMS

*(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 an on-line computer system on the accounting system and related internal controls and on audit procedures.

## On-Line Computer Systems

2.      On-line computer systems are computer systems that enable users to access data and programs directly through terminal devices. Such systems may comprise mainframe computers, minicomputers or a network of connected PCs. When the entity uses an on-line computer system, the technology is likely to be complex and linked with the entity's strategic business plans. The audit team may require special IT skills to make enquiries and to understand the implications of the responses obtained.[1] The auditors may need to consider using the work of an expert (see SAS 520 "Using the work of an expert").

3.      On-line systems allow users to directly initiate various functions such as:

   a.   entering transactions (for example, sales transactions in a retail store, cash withdrawals in a bank and shipment of goods in a plant);

   b.   making enquiries (for example, current customer account status or balance information);

   c.   requesting reports (for example, a list of inventory items with negative "on hand" quantities);

   d.   updating master-files (for example, setting up new customer accounts and changing general ledger codes); and

---

[1] See IEG 11 "Information Technology In The Accounting Curriculum" issued by the Education Committee of IFAC, which defines the broad content areas and specific knowledge and skills required by all professional accountants in connection with IT applied in a business context.

*(June 2003)*

e.  electronic commerce activities (for example, placing orders and paying for goods over the Internet).

4.  On-line computer systems use many different types of terminal devices. The functions they perform vary widely, and depend on their logic, transmission, storage and basic processing capabilities. Types of terminal devices are:

a.  general purpose terminals, such as:

   i.  basic keyboard and screen—used for entering data without any validation within the terminal and for displaying data from the computer system on the screen. For example, in entering a sales order, the main computer validates the product code and the terminal screen displays the result of the validation;

   ii.  intelligent terminal—used for the functions of the basic keyboard and screen with the additional functions of validating data within the terminal, maintaining transaction logs and performing other local processing. In the above sales order example, the intelligent terminal verifies the correct number of characters in the product code and the main computer verifies the existence of the product code in the master-file;

   iii.  PCs—used for all of the functions of an intelligent terminal with additional local processing and storage capabilities. Continuing the above example, the PC may perform all the verifications of the product code;

b.  special purpose terminals, such as:

   i.  point-of-sale devices—used to record sales transactions as they occur and to transmit them to the main computer. On-line cash registers and optical scanners used in the retail trade are typical point-of-sale devices;

   ii.  automated teller machines—used to initiate, validate, record, transmit and complete various banking transactions. Depending on the design of the system, certain of these functions are performed by the automated teller machine and others are performed on-line by the main computer;

   iii.  hand-held wireless devices for entering data from remote locations;

   iv.  voice response systems—used to allow user interaction with the computer over a telecommunications network based on verbal instructions issued by the computer. The customer communicates using a tone-generating device, which is often the keypad on the customer's telephone. Common applications include telephone banking and bill payment systems.

5.  Terminal devices may be found either locally or at remote sites. Local terminal devices are connected directly to the computer through cables, whereas remote terminal devices require the use of telecommunications to link them to the computer. In some cases, however, even local terminals may be connected using telecommunications links or wireless communication links. Terminal devices may be accessed by many users, for different purposes, in different locations, all at the same time. Users such as customers or suppliers may be within the entity or outside. In such cases, application software and data are kept on-line to meet users' needs. These systems also require other software, such as access control software and software that monitors on-line terminal devices.

6.  Increased sharing of system resources through LANs and WANs has led to the growth of distributed on-line processing. Client/Server systems have resulted in applications being split, so that processing can be performed across several machines. In a client/server environment,

the processing of data takes place on the server and the desktop computer (client).

7.    Employees, business partners, customers and other third parties may obtain access to an organization's on-line applications by using the Internet or other remote access services. External parties may access the organization's applications through electronic data interchange (EDI) or other electronic commerce applications.

8.    In addition to the users of these systems, programmers may use the on-line capabilities to develop new programs and maintain existing programs. Computer supplier personnel may also have on-line access to provide maintenance and support services.

## Types of On-Line Computer Systems

9.    On-line computer systems may be classified according to how information is entered into the system, how it is processed and when the results are available to the user. For purposes of this PN, on-line computer systems functions are classified as follows:

    a.   on-line/real-time processing;

    b.   on-line/batch processing;

    c.   on-line/memo update (and subsequent processing);

    d.   on-line/inquiry; and

    e.   on-line downloading/uploading processing.

### On-Line/Real-Time Processing

10.   In an on-line/real-time processing system, individual transactions are entered at terminal devices, validated and used to update related computer files immediately. An example is the application of cash receipts directly to customers' accounts. The results of such processing are then available immediately for inquiries or reports.

### On-Line/Batch Processing

11.   In a system with on-line input and batch processing, individual transactions are entered at a terminal device, subjected to certain validation checks and added to a transaction file that contains other transactions entered during the period. Later, during a subsequent processing cycle, the transaction file may be validated further and then used to update the relevant master-file. For example, journal entries may be entered and validated on-line and kept on a transaction file, with the general ledger master-file being updated on a monthly basis. Inquiries of, or reports generated from, the master-file will not include transactions entered after the last master-file update.

### On-Line/Memo Update (and Subsequent Processing)

12.   On-line input with memo update processing, also known as shadow update, combines on-line/real time processing and on-line/batch processing. Individual transactions immediately update a memo file containing information that has been extracted from the most recent version of the master-file. Inquiries are made from this memo file. These same transactions are added to a transaction file for subsequent validation and updating of the master-file on a batch basis. For example, the withdrawal of cash through an automated teller machine is checked against the customer's balance on the memo file, and is then immediately posted to the customer's account on that file to reduce the balance by the amount of the withdrawal. From the user's perspective, this system will seem no different from on-line/real

time processing since the results of data entered are available immediately. However, the transactions have not been subjected to complete validation before the master-file update.

### On-Line/Inquiry

13. On-line inquiry restricts users at terminal devices to making inquiries of master-files. In such systems, the master-files are updated by other systems, usually on a batch basis. For example, the user may inquire of the credit status of a particular customer before accepting an order from that customer.

### On-Line Downloading/Uploading Processing

14. On-line downloading refers to the transfer of data from a master-file to an intelligent terminal device for further processing by the user. For example, data at the head office representing transactions of a branch may be downloaded to a terminal device at the branch for further processing and preparation of branch financial reports. The results of this processing and other locally processed data may then be uploaded to the head office computer.

## Characteristics of On-Line Computer Systems

15. The characteristics of on-line computer systems may apply to many of the types of on-line systems discussed in the previous section. The most significant characteristics relate to on-line data entry and validation, on-line access to the system by users, possible lack of visible transaction trail and potential access to the system by non-users, including programmers and other third parties (for example, through e-mail and the Internet). The particular characteristics of a specific on-line system will depend on the design of that system.

16. When data are entered on-line, they are usually subject to immediate validation checks. Data failing this validation are not accepted and a message may be displayed on the terminal screen, providing the user with the ability to correct the data and re-enter the valid data immediately. For example, if the user enters an invalid inventory part number, an error message is displayed, allowing the user to re-enter a valid part number.

17. Users may have on-line access to the system that enables them to perform various functions (for example, to enter transactions and to read, change or delete programs and data files through the terminal devices). Unlimited access to all of these functions in a particular application is undesirable because it provides the user with the potential ability to make unauthorized changes to the data and programs. Unlimited access precludes segregation of duties and allows users access to all stages of processing and recording a transaction. The extent of this access depends on things such as the design of the particular application and the implementation of software designed to control access to the system.

18. An on-line computer system may be designed not to provide supporting documents for all transactions entered into the system. Such a system must be able to provide details of the transactions on request or by transaction logs or other means. Examples of these types of systems include orders received by a telephone operator who enters them on-line without written purchase orders, and cash withdrawals from automated teller machines.

19. Programmers may have on-line access to the system that enables them to develop new programs and modify existing programs. Unrestricted access provides the programmer with the potential to make unauthorized changes to programs and obtain unauthorized access to other parts of the system and would represent a serious control weakness. The extent of this access depends on the requirements of the system. For example, in some systems, programmers ordinarily have access only to programs maintained in a separate program development and maintenance library. Programmers may, however, be authorized to change the operational programs in emergencies that require changes to programs kept on-line. In

such cases, formal control procedures would be followed after the emergency to ensure appropriate authorization and documentation of the changes.

## Internal Control in an On-Line Computer System

20.  Applications in an on-line environment may have greater exposure to unauthorized access and update. An entity's security infrastructure plays an important part in ensuring the integrity of the information produced. The auditors, therefore, consider the security infrastructure before examining the general and application controls. The entity may need to establish suitable general controls to mitigate the risks of viruses, unauthorized access and the potential destruction of audit trails. Hence access controls are particularly important to on-line processing.

21.  These controls may include the use of passwords and specialized access control software, such as on-line monitors, that maintains control over the menus, authorization tables, passwords, files and programs that users are permitted to access. They may also include physical controls such as the use of key locks on terminal devices, locked computer rooms and inactivity timeouts. Other important aspects of control in an on-line computer system include:

   a.  controls over passwords: procedures for the assignment and maintenance of passwords to restrict access to authorized users;

   b.  system development and maintenance controls: additional procedures to ensure that controls essential to on-line applications, such as passwords, access controls, on-line data validation and recovery procedures, are included in the system during its development and maintenance; the controls are also designed to ensure that changes to systems operate as expected and are made in the correct manner;

   c.  programming controls;

   d.  transaction logs; and

   e.  firewalls.

22.  Certain application controls are particularly important to on-line processing. These include the following:

   a.  Pre-processing authorization. Authorization to initiate a transaction, for example, by using a bank card together with a personal identification number before being able to make a cash withdrawal through an automated teller machine.

   b.  Terminal device edit, reasonableness and other validation tests. Programmed routines that check the input data and processing results for completeness, accuracy and reasonableness. These routines include sequence, limit, range and reasonableness checks and may be performed on an intelligent terminal device or on the central computer.

   c.  Input error reporting and handling. Procedures to ensure that all input errors are properly reported, identified and rejected from further processing, corrected and resubmitted for processing in a timely manner. These procedures will generally comprise a mix of both manual and automated routines.

   d.  Cut-off procedures. Procedures that ensure transactions are processed in the proper accounting period. These are particularly necessary in systems that have a continuous flow of transactions. For example, in on-line systems where terminal devices in various locations record sales orders and shipments, there is a need to coordinate the actual

shipment of goods, inventory release and invoice processing.

e.  File controls. Procedures that ensure the correct data files are used for on-line processing.

f.  Master file controls. Changes to master-files are controlled by procedures similar to those used for controlling other input transaction data. More stringent enforcement of these control procedures may be necessary because master file data may have a pervasive effect on processing results.

g.  Balancing. The process of establishing control totals over data being submitted for processing through the on-line terminal devices and comparing the control totals during and after processing to ensure that complete and accurate data are transferred to each processing phase. These balancing controls are important to monitoring completeness and accuracy controls in a real-time processing environment. They should be included in the automated program routines whenever possible.

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

   i.    receives all data for processing;

   ii.   ensures that all data are authorized and recorded;

   iii.  follows up all errors detected during processing;

   iv.   verifies the proper distribution of output; and

   v.    restricts physical access to application programs and data.

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

**Effect of On-Line Computer Systems on the Accounting System and Related Internal Controls**

23.  The effect of an on-line computer system on the accounting system and the associated risks will generally depend on:

   a.  the extent to which the on-line system is being used to process accounting applications;

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

   c.  the nature of files and programs the applications use.

The entity's security infrastructure plays an important part in controlling the effect of the risks created by the entity's use of an on-line environment.

24.  Factors such as the following may reduce the risk of errors occurring because of the entity's use of on-line systems:

   a.  Performing data entry at or near the point where transactions originate reduces the risk that the transactions will not be recorded.

   b.  Immediate correction and re-entering of invalid transactions reduces the risk that such transactions will not be corrected and resubmitted quickly.

   c.  Data entry performed by individuals who understand the nature of the transactions involved may be less prone to error than when performed by individuals unfamiliar with the nature of the transactions.

d.  Processing transactions immediately reduces the risk that they will be processed in the wrong accounting period.

e.  Authentication and authorization carried out at or near the point where transactions originate reduces the risk of impersonation or other unauthorized access to or manipulation of data.

25.  The risk of errors in on-line computer systems may be increased for the following reasons:

a.  Locating terminal devices throughout the entity increases the opportunity for unauthorized use of a terminal device and the entry of unauthorized transactions.

b.  On-line terminal devices may provide easier opportunity for unauthorized uses such as:

i.  Modification of previously entered transactions or balances;

ii.  Modification of computer programs; or

iii.  Access to data and programs from remote locations.

c.  If on-line processing is interrupted for any reason, for example, due to faulty telecommunications, there may be a greater chance that transactions or files may be lost and that the recovery may not be accurate and complete.

d.  On-line access to data and programs from remote sites through telecommunications may provide greater opportunity for access to data and programs by unauthorized persons. Organizations that have links to the Internet require greater controls, such as firewalls, to manage the risk of unauthorized access to data and programs.

e.  The use of electronic commerce and EDI for the exchange of documents between two organizations results in the loss of traditional paper audit trails, including invoices and purchase orders.

26.  The characteristics of on-line computer systems, as described earlier in this PN, illustrate some of the considerations influencing the effectiveness of controls in on-line computer systems. Such characteristics may have the following consequences:

a.  there may not be printed source documents for every input transaction;

b.  results of processing may be highly summarized; for example, only totals from individual on-line data entry devices can be traced to subsequent processing;

c.  the on-line computer system may not be designed to provide printed reports; for example, edit reports may be replaced by edit messages displayed on a terminal device screen;

d.  on-line computer systems running real-time processes pose particular difficulties for auditors as it can be difficult to achieve a clear cut-off of data. It can also be difficult in some IT environments to stop real-time processing long enough to obtain copies of data files or to run important reports for audit purposes at period end; and

e.  in the event that real time systems have to be restored, it is difficult to ensure that all of the data is properly reinstated and, importantly, that all systems integration interfaces and data feeds are reset to the date and time of the back-up data.

**Effect of On-Line Computer Systems on Audit Procedures**

27. Generally, in a well-designed and controlled on-line computer system, it is likely that the auditors will test general and application controls. If those controls are deemed satisfactory, the auditors will place greater reliance on internal controls in the system when determining the nature timing and extent of audit procedures. The characteristics of on-line computer systems may make it more effective for the auditors to perform a pre-implementation review of new on-line accounting applications rather than to review the applications after installation. To be fully effective, the review may need to extend to other applications that provide data for those accounting applications; the auditors may also test that the new system operates and is implemented as designed. The pre-implementation review may provide the auditors with an opportunity to request additional functions, such as detailed transaction listings, or controls within the application design. It may also provide the auditors with sufficient time to develop and test audit procedures in advance of the system's use. In contrast, when the entity adopts a policy of continuous systems' upgrading, the change management procedures adopted may be critical to the on-going effectiveness of the controls in place. The auditors may therefore examine the change management procedures rather than perform pre-implementation reviews.

28. The following matters are of particular importance to the auditors in an on-line computer system:

    a. authorization, completeness and accuracy of on-line transactions through the implementation of appropriate controls at the time when the transaction is accepted for processing;

    b. integrity of records and processing, due to many users and programmers having on-line access to the system; and

    c. necessary changes in the performance of audit procedures, including the use of CAATs (see PN 1009 "Computer-Assisted Audit Techniques"), due to matters such as:

        i. the need for audit teams with technical skills in on-line computer systems;

        ii. the effect of the on-line computer system on the timing of audit procedures;

        iii. the lack of visible transaction trails;

        iv. procedures carried out during the audit planning stage (see paragraph 29);

        v. audit procedures performed concurrently with on-line processing (see paragraph 30); and

        vi. procedures performed after processing has taken place (see paragraph 31).

29. Procedures carried out during the planning stage may include the following:

    a. the participation on the audit team of individuals with technical proficiency in on-line computer systems and related controls;

    b. identification of any new remote access facilities; and

    c. preliminary determination, during the risk assessment process, of the impact of the system on the audit procedures.

30.     Audit procedures performed concurrently with on-line processing may include tests of the controls over the on-line applications. For example, this may be by means of entering test transactions through the on-line terminal devices or by the use of audit software. These tests may be used either to confirm the auditors' understanding of the system or to test controls such as passwords and other access controls. Where the entity permits access through the Internet, audit procedures can include tests of firewalls and other authorization and access controls, as well as tests of transaction processing. To avoid the inadvertent corruption of client records, the auditors review concurrent procedures with appropriate client personnel and obtains approval before conducting the tests.

31.     Procedures performed after processing has taken place may include the following:

    a.  tests of controls over transactions logged by the on-line system for authorization, completeness and accuracy;

    b.  substantive procedures covering transactions and processing results rather than tests of control, where the former may be more cost-effective or where the system is not well-designed or controlled; and

    c.  reprocessing transactions as either a test of control or a substantive procedure.


## Compatibility with International Auditing Practice Statements

32.     This Practice Note is, in all material respects, in accordance with International Auditing Practice Statement 1002 "IT Environments – On-Line Computer Systems".