PRACTICE NOTE

1003

IT ENVIRONMENTS – DATABASE 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 a database system on the accounting system and related internal controls and on audit procedures.

2. A database is a collection of data that is shared and used by many different users for different purposes. Each user may not necessarily be aware of all the data stored in the database, or of the ways that the data may be used for multiple purposes. Generally, individual users are aware only of the data that they use and may view the data as computer files utilized by their applications.

3. When an entity uses a database system, the technology is likely to be complex and may be linked with the entity's strategic business plans. The audit team may require special IT skills to make appropriate inquiries and to understand the implications of the responses obtained[1]. The auditor may need to consider using the work of an expert (see SAS 520 "Using the work of an expert").

Database Systems

4. Database systems consist principally of two components: the database and the database management system (DBMS). Database systems interact with other hardware and software aspects of the overall computer system.

5. The software that creates, maintains and operates the database is referred to as DBMS software. Together with the operating system, the DBMS facilitates the physical storage of the data, maintains the interrelationships between the data, and makes the data available to application programs. It also provides controlled access methods to establish basic security measures over the data. Usually, the DBMS software is supplied by a commercial vendor but

---

[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.

will need to be adapted to the entity's needs.

6.   The guidance in this PN applies to database systems used in multiple user environments. Although database systems may reside on any type of computer system, including PCs, this PN does not relate to PC environments with only a single user.

Database System Characteristics

7.   Database systems are distinguished by two important characteristics: data sharing and data independence. These characteristics ordinarily require the use of a data dictionary (paragraph 11) and the establishment of a data resource management (paragraphs13-19).

Data Sharing

8.   A database is composed of data set up with defined relationships and organized to permit many users to use the data in different application programs. Individual applications share the data in the database for different purposes. For example, an inventory item unit cost maintained by the database may be used by one application program to produce a cost of sales report and by another program to prepare an inventory valuation.

Data Independence from Application Programs

9.   The DBMS records the data once for use by various application programs. This creates a need for data sharing and a need for data independence from application programs. In non-database systems, separate data files are maintained for each application. Similar data used by several applications may be repeated in several different files. In a database system, however, a single file of data (or database) is used by many applications, with data redundancy kept to a minimum.

10.   DBMSs differ in the degree of data independence they provide. The degree of data independence is related to the ease with which personnel can make changes to application programs or to the database. True data independence is achieved when the structure of data in the database can be changed without affecting the application programs, and *vice versa*.

Data Dictionary

11.   A significant implication of data sharing and data independence is the potential for the recording of data only once for use in several applications. Because various application programs need to access these data, a software facility is required to keep track of the location of the data in the database. This software within the DBMS is known as a data dictionary. It also serves as a tool to maintain standardized documentation and definitions of the database environment and application systems. A data dictionary provides functions such as:

   a.   a facility to create or modify data definitions;

   b.   validation of the data definitions provided to ensure their integrity;

   c.   prevention of unauthorized access or manipulations of the data definitions; and

   d.   interrogation and reporting facilities that allow the database administrator to make inquires on the data definitions.

12.   Databases may be structured as flat file databases, or as relational databases. In a flat file database, all the data concerning one record are stored as part of that record. With a relational database, data are stored as a series of tables, with links between the tables as necessary. Relational databases minimize the duplication of stored data, as data shared by more than one

record need to be stored only once. The data themselves may comprise objects for use with object-oriented applications. This can lead to complicated data structures.

Data Resource Management

13.   Data resource management forms an essential organizational control in ensuring data integrity and compatibility. In a database environment the methods of informational control and usage change from an application-orientated approach to an organization-wide approach. In contrast to traditional systems where each application is a separate system with its own reporting and controls, in a database environment, many controls may be centralized and the database is designed to serve the entire information needs of the organization.

14.   The use of the same data by various application programs emphasizes the importance of centralized coordination of the use and definition of data and the maintenance of their integrity, security, accuracy and completeness. Data resource management is required to promote data integrity for the organization as a whole and includes a data administration function (refer to paragraph 15) and a database administration function (refer to paragraphs 16-19). The data administration function is concerned with the "ownership" of data, its meaning, and its relationship with other data and its entity-wide integrity. In contrast, the database administration function is primarily concerned with the technical implementation of the database, the day-to-day operations of the database and the policies and procedures governing its access and everyday usage.

Data Administration

15.   The data administration function manages data as an organizational resource and includes responsibilities for:

   a.   the development and implementation of a data resource management strategic plan and policies, which support the entity's business plans by achieving cost-effective use of the organization's data;

   b.   the creation and maintenance of a corporate data model or architecture (sometimes referred to as an enterprise data model);

   c.   the coordination and integration of system data models;

   d.   obtaining agreement among users about definitions and format of data;

   e.   resolving conflicts about incompatible representation and data;

   f.   establishing a corporate-wide data dictionary and managing the organization's naming and definition standards;

   g.   establishing data standards and procedures for:

      i.   data naming;

      ii.   data usage;

      iii. data security;

      iv.   data definition compilation; and

      v.   data modeling; and

h. providing training and consulting to users and the data information technology team members (system developers and database administrators) concerning all aspects of data resource management.

Database Administration

16. Coordination is usually the responsibility of a group of individuals who are typically referred to as "database administration." The individual who heads this function may be referred to as the "database administrator." Generally, the database administration function takes responsibility for the definition, structure, security, operational control and efficiency of databases, including the definition of the rules for accessing and storing data.

17. Database administration tasks may also be performed by individuals who are not part of a centralized database administration group. When the tasks of database administration are distributed among existing organizational units rather than being centralized, the different tasks still need to be coordinated.

18. Database administration tasks typically include:

a. defining the database structure and the description of the data model. Determining how data are defined, stored and accessed by users of the database to ensure that all their requirements are met on a timely basis;

b. maintaining data integrity, security and completeness. Developing, implementing and enforcing the rules for data integrity, completeness and access. Responsibilities include:

i. defining who is responsible for monitoring the appropriate origin of data and how such monitoring is performed;

ii. defining who may access data and how the access is accomplished (for example, through passwords and authorization tables);

iii. preventing the inclusion of incomplete or invalid data;

iv. detecting the absence of data;

v. securing the database from unauthorized access and destruction;

vi. monitoring and follow-up of security incidents and regular backing-up of data; and

vii. arranging total recovery in the event of a loss. In such a circumstance, the backup protocol covering the data tables is likely to be complex;

c. coordinating computer operations related to the database. Assigning responsibility for physical computer resources and monitoring their use relative to the operation of the database;

d. monitoring system performance. Developing performance measures to monitor the integrity of the data, the ability of the database to respond to the needs of users and the frequency of data changes and access; and

e. providing administrative support. Coordinating and liaising with the vendor of the DBMS, assessing new releases issued by the vendor of the DBMS and the extent of their effect on the entity, installing new releases and ensuring that appropriate internal education is provided.

19. Some applications may use more than one database. In these circumstances, the tasks of the database administration group will include the need to ensure:

a. adequate linkage between databases;

b. coordination of functions; and

c. consistency between data in different databases.

Internal Control in a Database Environment

20. Because an entity's security infrastructure plays an important part in ensuring the integrity of the information produced, the auditors consider that infrastructure before examining the general and application controls. Generally, internal control in a database environment requires effective controls over the database, the DBMS and the applications. The effectiveness of internal controls depends very much on the nature of data administration and the database administration tasks (paragraphs 15-19), and on how they are performed.

21. In database systems, general controls normally have a greater influence than application controls because of data sharing, data independence and other characteristics of database systems. General controls over the database, the DBMS and the activities of the data resource management (data administration and database administration) have a pervasive effect on application processing. As paragraph 29 notes, the use of a DBMS and the functions built into it can help to provide effective controls. The general controls of particular importance in a database environment can be classified into the following groups:

a. standard approach for development and maintenance of application programs;

b. data model and data ownership;

c. access to the database;

d. segregation of duties;

e. data resource management; and

f. data security and database recovery.

Standard Approach for Development and Maintenance of Application Programs

22. Since many users share the data, using a standard approach to develop each new application program and to modify existing application programs may enhance control. This includes a formalized, step-by-step approach all individuals must follow when developing or modifying an application program. It also includes analyzing the effect of new and existing transactions on the database each time a modification is required. The resulting analysis would indicate the effects of the changes on the security and integrity of the database. Implementing a standard approach to develop and modify application programs is a technique that can help improve the accuracy, integrity and completeness of the database. The following are some of the controls that can help to achieve this:

a. definition standards are established and monitored for compliance.

b. data backup and recovery procedures are established and implemented to ensure database availability;

    c. various levels of access control for data items, tables and files are established to prevent inadvertent or unauthorized access;

    d. controls are established to ensure accuracy, completeness and consistency of data elements and relationships in the database. However, in complex systems, the systems design may not always provide users with controls that prove the completeness and accuracy of data and there may be increased risk that the DBMS will not always identify data or index corruptions; and

    e. database restructuring procedures are followed when making logical, physical and procedural changes.

Data Model and Data Ownership

23.   In a database environment, where many individuals may use programs to input and modify data, the database administrator needs to ensure there is a clear and definite assignment of responsibility for the accuracy and integrity of each item of data. A single data owner should be assigned responsibility for defining access and security rules, such as who can use the data (access) and what functions they can perform (security). Assigning specific responsibility for data ownership helps to ensure the integrity of the database. For example, the credit manager may be the designated "owner" of a customer's credit limit and would be responsible for determining the authorized users of that information. If several individuals are able to make decisions affecting the accuracy and integrity of given data, the likelihood increases of the data becoming corrupted or improperly used. The controls over user profiles are also important when using a database system, not only to establish authorized access but also, to detect violations or attempted violations.

Access to the Database

24.   User access to the database can be restricted through access controls. These restrictions apply to individuals, terminal devices and programs. For passwords to be effective, adequate procedures are required for changing passwords, maintaining the secrecy of passwords, and reviewing and investigating attempted security violations. Relating passwords to defined terminal devices, programs and data helps to ensure that only authorized users and programs can access, amend or delete data. For example, the credit manager may give sales clerks authority to refer to a customer's credit limit, whereas a warehouse clerk might not have such authorization.

25.   The use of authorization tables may further control user access to the various elements of the database. Improper implementation of access procedures can result in unauthorized access to the database. Appropriate controls also ensure that data stored is convertible into a human-readable format within a reasonable time.

Segregation of Duties

26.   The responsibilities for performing the various activities required to design, implement and operate a database are divided among technical, design, administrative and user personnel. Their duties include system design, database design, administration and operation. Maintaining adequate segregation of these duties is necessary to ensure the completeness, integrity and accuracy of the database. For example, individuals responsible for modifying personnel database programs should not be the same ones who are authorized to change individual pay rates in the database.

Data Security and Database Recovery

27.   Databases are likely to be used by people in many different parts of an entity's operations. This means that many parts of the entity would be affected if the data were unavailable or

contained errors. Accordingly, the general controls for data security and database recovery assume a high level of importance in database systems.

The Effect of Databases on the Accounting System and Related Internal Controls

28.   The effect of a database system on the accounting system and the associated risks will generally depend on factors such as:

    a. the extent to which databases are being used by accounting applications;

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

    c. the nature and structure of the database, the DBMS (including the data dictionary), the database administration tasks and the applications (for example, batch or on-line update); and

    d. the general and application controls that are particularly important in a database environment.

29.   Database systems typically provide the opportunity for greater reliability of data than non-database systems. In such systems general controls assume a greater importance than application controls. This can result in reduced risk of fraud or error in accounting systems where databases are used. The following factors, combined with adequate controls, contribute to this improved reliability of data.

    a. Improved consistency of data is achieved because data are recorded and updated only once, rather than being stored in several files and updated at different times and by different programs.

    b. Integrity of data will be improved by effective use of facilities included in the DBMS, such as recovery/restart routines, generalized edit and validation routines, and security and control features.

    c. Other functions available with the DBMS can facilitate control and audit procedures. These functions include report generators, which may be used to create balancing reports, and query languages, which may be used to identify inconsistencies in the data.

30.   Alternatively, the risk of misstatement may increase if database systems are used without adequate controls. In a typical non-database environment, controls exercised by individual users may compensate for weaknesses in general controls. In a database system, however, individual users cannot always compensate for inadequate database administration controls. For example, accounts receivable personnel cannot effectively control accounts receivable data if other personnel are not restricted from modifying accounts receivable balances in the database.

The Effect of Databases on Audit Procedures

31.   Audit procedures in a database environment will be affected principally by the extent to which the accounting system uses the data in the database. Where significant accounting applications use a common database, the auditors may find it cost-effective to use some of the procedures in the following paragraphs.

32.   To obtain an understanding of the database control environment and the flow of transactions the auditors may consider the effect of the following on audit risk in planning the audit.

a. The relevant access controls. People outside the traditional accounting function may use the databases, and the auditors consider the access controls over accounting data and all those who may have access to it.

b. The DBMS and the significant accounting applications using the database. Other applications within the entity may generate or alter data the accounting applications use. The auditors consider how the DBMS controls these data.

c. The standards and procedures for development and maintenance of application programs using the database. Databases, especially those on stand-alone computers, may often be designed and implemented by people outside the IT or accounting functions. The auditors consider how the entity controls the development of these databases.

d. The data resource management function. As discussed in paragraphs13-19, this function plays an important role in maintaining the integrity of data stored on the database.

e. Job descriptions, standards and procedures for those individuals responsible for technical support, design, administration and operation of the database. With database systems, it is likely that a wider range of individuals have significant data responsibilities than would be the case with non-database systems.

f. The procedures used to ensure the integrity, security and completeness of the financial information contained in the database.

g. The availability of audit facilities within the DBMS.

h. The procedures used to introduce new versions of the database into operation.

33. When determining the extent of reliance on internal controls related to the use of databases in the accounting system The auditors may consider how the controls described in paragraphs 22-27 are used. If the auditors subsequently decide to rely on those controls, the auditors design and perform appropriate tests.

34. When the auditors decide to perform tests of control or substantive procedures related to the database system, it will often be more effective to do so using computer assisted audit techniques. The fact that the data are all stored in one place and organized in a consistent manner makes extraction of samples easier. Also, databases may include data generated outside the accounting function, which will help make the application of analytical procedures more effective.

35. Audit procedures may include using the functions of the DBMS to:

a. test access controls;

b. generate test data;

c. provide an audit trail;

d. check the integrity of the database;

e. provide access to the database or a copy of relevant parts of the database to enable the use of audit software (see PN 1009 "Computer-Assisted Audit Techniques"); and

f. obtain information necessary for the audit.

Before using the DBMS facilities, the auditors consider whether they are functioning adequately.

36.   If the database administration controls are inadequate, the auditors may not be able to compensate for weak controls by any amount of substantive work. Therefore, when it becomes clear that the controls in the database system cannot be relied on, the auditors consider whether performing substantive procedures on all significant accounting applications that use the database would achieve the audit objective. If the auditors are unable to overcome the weakness in the control environment with substantive work to reduce audit risk to an acceptably low level, SAS 600 "Auditors' reports on financial statements" requires the auditors to qualify or disclaim an opinion.

37.   The characteristics of database systems may make it more effective for the auditors to perform a pre-implementation review of new accounting applications rather than to review the applications after installation. This pre-implementation review and review of the change management process may provide the auditors with an opportunity to request additional functions, such as built-in audit routines 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.

Compatibility with International Auditing Practice Statements

38.   This Practice Note is, in all material respects, in accordance with International Auditing Practice Statement 1003 "IT Environments – Database Systems".