EXPOSURE DRAFT ISSUED FOR CONSULTATION UNTIL 5 SEPTEMBER 2003

PRACTICE NOTE

1013

ELECTRONIC COMMERCE – EFFECT ON THE AUDIT OF FINANCIAL STATEMENTS

(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. The purpose of this Practice Note (PN) is to provide guidance to assist auditors of financial statements where an entity engages in commercial activity that takes place by means of connected computers over a public network, such as the Internet (e-commerce[1]). The guidance in this PN is particularly relevant to the application of SAS 200 "Planning", SAS 210 "Knowledge of the business" and SAS 300 "Audit risk assessments and accounting and internal control systems".

2. This PN identifies specific matters to assist the auditors when considering the significance of e-commerce to the entity's business activities and the effect of e-commerce on the auditors' assessments of risk for the purpose of forming an opinion on the financial statements. The purpose of the auditors' consideration is not to form an opinion or provide consulting advice concerning the entity's e-commerce systems or activities in their own right.

3. Communications and transactions over networks and through computers are not new features of the business environment. For example, business processes frequently involve interaction with a remote computer, the use of computer networks, or electronic data interchange (EDI). However the increasing use of the Internet for business to consumer, business to business, business to government and business to employee e-commerce is introducing new elements of risk to be addressed by the entity and considered by the auditors when planning and performing the audit of the financial statements.

4. The Internet refers to the worldwide network of computer networks, it is a shared public network that enables communication with other entities and individuals around the world. It is interoperable, which means that any computer connected to the Internet can communicate with any other computer connected to the Internet. The Internet is a public network, in

[1] The term e-commerce is used in this PN. E-business is also commonly used in a similar context. There are no generally accepted definitions of these terms, and e-commerce and e-business are often used interchangeably. Where a distinction is made, e-commerce is sometimes used to refer solely to transactional activities (such as the buying and selling of goods and services) and e-business is used to refer to all business activities, both transactional and non-transactional, such as customer relations and communications.

contrast to a private network that only allows access to authorized persons or entities. The use of a public network introduces special risks to be addressed by the entity. Growth of Internet activity without due attention by the entity to those risks may affect the auditors' assessment of risk.

5. While this PN has been written for situations where the entity engages in commercial activity over a public network such as the Internet, much of the guidance it contains can also be applied when the entity uses a private network. Similarly, while much of this guidance will be helpful when auditing entities formed primarily for e-commerce activities (often called "dot coms") it is not intended to deal with all audit issues that would be addressed in the audit of such entities.

Skills and Knowledge

6. The level of skills and knowledge required to understand the effect of e-commerce on the audit will vary with the complexity of the entity's e-commerce activities. The auditors consider whether the personnel assigned to the engagement have appropriate IT[2] and Internet business knowledge to perform the audit. When e-commerce has a significant effect on the entity's business, appropriate levels of both information technology (IT) and Internet business knowledge may be required to:

   a. understand, so far as they may affect the financial statements:

      i. the entity's e-commerce strategy and activities;

      ii. the technology used to facilitate the entity's e-commerce activities and the IT skills and knowledge of entity personnel; and

      iii. the risks involved in the entity's use of e-commerce and the entity's approach to managing those risks, particularly the adequacy of the internal control system, including the security infrastructure and related controls, as it affects the financial reporting process;

   b. determine the nature, timing and extent of audit procedures and evaluate audit evidence; and

   c. consider the effect of the entity's dependence on e-commerce activities on its ability to continue as a going concern.

7. In some circumstances, the auditors may decide to use the work of an expert, for example if the auditors consider it appropriate to test controls by attempting to break through the security layers of the entity's system (vulnerability or penetration testing). When the work of an expert is used, the auditors obtain sufficient appropriate audit evidence that such work is adequate for the purposes of the audit, in accordance with SAS 520 "Using the work of an expert". The auditors also consider how the work of the expert is integrated with the work of others on the audit, and what procedures are undertaken regarding risks identified through the expert's work.

Knowledge of the Business

8. SAS 210 "Knowledge of the business" requires that the auditors obtain a knowledge of the

[2] International Education Guideline IEG 11, "Information Technology in the Accounting Curriculum" issued by the Education Committee of IFAC, which defines the broad content areas and specific skills and knowledge required by all professional accountants in connection with IT applied in a business context, may assist the auditors in identifying appropriate skills and knowledge.

business sufficient to enable the auditors to identify and understand the events, transactions and practices that may have a significant effect on the financial statements or on the audit report. Knowledge of the business includes a general knowledge of the economy and the industry within which the entity operates. The growth of e-commerce may have a significant effect on the entity's traditional business environment.

9. The auditors' knowledge of the business is fundamental to assessing the significance of e-commerce to the entity's business activities and any effect on audit risk. The auditors consider changes in the entity's business environment attributable to e-commerce, and e-commerce business risks as identified so far as they affect the financial statements. Although the auditors obtain much information from enquiries of those responsible for financial reporting, making enquiries of personnel directly involved with the entity's e-commerce activities, such as the Chief Information Officer or equivalent, may also be useful. In obtaining or updating knowledge of the entity's business, the auditors consider, so far as they affect the financial statements:

   a. the entity's business activities and industry (paragraphs 10-12);

   b. the entity's e-commerce strategy (paragraph 13);

   c. the extent of the entity's e-commerce activities (paragraphs 14-16); and

   d. the entity's outsourcing arrangements (paragraphs 17-18).

   Each of these is discussed below.

The Entity's Business Activities and Industry

10. E-commerce activities may be complementary to an entity's traditional business activity. For example, the entity may use the Internet to sell conventional products (such as books or CDs), delivered by conventional methods from a contract executed on the Internet. In contrast, e-commerce may represent a new line of business and the entity may use its web site to both sell and deliver digital products via the Internet.

11. The Internet lacks the clear, fixed geographic lines of transit that traditionally have characterized the physical trade of many goods and services. In many cases, particularly where goods or services can be delivered via the Internet, e-commerce has been able to reduce or eliminate many of the limitations imposed by time and distance.

12. Certain industries are more conducive to the use of e-commerce, therefore e-commerce in these industries is in a more mature phase of development. When an entity's industry has been significantly influenced by e-commerce over the Internet, business risks that may affect the financial statements may be greater. Examples of industries that are being transformed by e-commerce include:

   a. computer software;

   b. securities trading;

   c. banking;

   d. travel services;

   e. books and magazines;

   f. recorded music;

g. advertising;

h. news media; and

i. education.

In addition many other industries, in all business sectors, have been significantly affected by e-commerce.

The Entity's E-Commerce Strategy

13. The entity's e-commerce strategy, including the way it uses IT for e-commerce and its assessment of acceptable risk levels, may affect the security of the financial records and the completeness and reliability of the financial information produced. Matters that may be relevant to the auditors when considering the entity's e-commerce strategy in the context of the auditors' understanding of the control environment, include:

a. involvement of those charged with governance in considering the alignment of e-commerce activities with the entity's overall business strategy;

b. whether e-commerce supports a new activity for the entity, or whether it is intended to make existing activities more efficient or reach new markets for existing activities;

c. sources of revenue for the entity and how these are changing (for example, whether the entity will be acting as a principal or agent for goods or services sold);

d. management's evaluation of how e-commerce affects the earnings of the entity and its financial requirements;

e. management's attitude to risk and how this may affect the risk profile of the entity;

f. the extent to which management has identified e-commerce opportunities and risks in a documented strategy that is supported by appropriate controls, or whether e-commerce is subject to ad hoc development responding to opportunities and risks as they arise; and

g. management's commitment to relevant codes of best practice or web seal programs.

The Extent of the Entity's E-commerce Activities

14. Different entities use e-commerce in different ways. For example, e-commerce might be used to:

a. provide only information about the entity and its activities, which can be accessed by third parties such as investors, customers, suppliers, finance providers, and employees;

b. facilitate transactions with established customers whereby transactions are entered via the Internet;

c. gain access to new markets and new customers by providing information and transaction processing via the Internet;

d. access Application Service Providers (ASPs); and

e. create an entirely new business model.

15. The extent of e-commerce use affects the nature of risks to be addressed by the entity. Security issues may arise whenever the entity has a web site. Even if there is no third party

interactive access, information-only pages can provide an access point to the entity's financial records. The security infrastructure and related controls can be expected to be more extensive where the web site is used for transacting with business partners, or where systems are highly integrated (see paragraphs 32-34).

16. As an entity becomes more involved with e-commerce, and as its internal systems become more integrated and complex, it becomes more likely that new ways of transacting business will differ from traditional forms of business activity and will introduce new types of risks.

The Entity's Outsourcing Arrangements

17. Many entities do not have the technical expertise to establish and operate in-house systems needed to undertake e-commerce. These entities may depend on service organizations such as Internet Service Providers (ISPs), Application Service Providers (ASPs) and data hosting companies to provide many or all of the IT requirements of e-commerce. The entity may also use service organizations for various other functions in relation to its e-commerce activities such as order fulfillment, delivery of goods, operation of call centers and certain accounting functions.

18. When the entity uses a service organization, certain policies, procedures and records maintained by the service organization may be relevant to the audit of the entity's financial statements. The auditors consider the outsourcing arrangements used by the entity to identify how the entity responds to risks arising from the outsourced activities. SAS 480 "Audit considerations relating to entities using service organizations" provides guidance on assessing the effect that the service entity has on control risk.

Risk Identification

19. Management faces many business risks relating to the entity's e-commerce activities, including:

    a. loss of transaction integrity, the effects of which may be compounded by the lack of an adequate audit trail in either paper or electronic form;

    b. pervasive e-commerce security risks, including virus attacks and the potential for the entity to suffer fraud by customers, employees and others through unauthorized access;

    c. improper accounting policies related to, for example, capitalization of expenditures such as website development costs, misunderstanding of complex contractual arrangements, title transfer risks, translation of foreign currencies, allowances for warranties or returns, and revenue recognition issues such as:

        i. whether the entity is acting as principal or agent and whether gross sales or commission only are to be recognized;

        ii. if other entities are given advertising space on the entity's web site, how revenues are determined and settled (for example, by the use of barter transactions);

        iii. the treatment of volume discounts and introductory offers (for example, free goods worth a certain amount);

        iv. cut off (for example, whether sales are only recognized when goods and services have been supplied);

    d. noncompliance with taxation and other legal and regulatory requirements, particularly when Internet e-commerce transactions are conducted across international boundaries;

e. failure to ensure that contracts evidenced only by electronic means are binding;

f. over reliance on e-commerce when placing significant business systems or other business transactions on the Internet; and

g. systems and infrastructure failures or "crashes".

20. The entity addresses certain business risks arising in e-commerce through the implementation of an appropriate security infrastructure and related controls, which generally include measures to:

a. verify the identity of customers and suppliers;

b. ensure the integrity of transactions;

c. obtain agreement on terms of trade, including agreement of delivery and credit terms and dispute resolution processes, which may address tracking of transactions and procedures to ensure a party to a transaction cannot later deny having agreed to specified terms (non-repudiation procedures);

d. obtain payment from, or secure credit facilities for, customers; and

e. establish privacy and information protection protocols.

21. The auditors use the knowledge of the business obtained to identify those events, transactions and practices related to business risks arising from the entity's e-commerce activities that, in the auditors' judgment, may result in a material misstatement of the financial statements or have a significant effect on the auditors' procedures or the audit report.

Legal and Regulatory Issues

22. A comprehensive international legal framework for e-commerce and an efficient infrastructure to support such a framework (electronic signatures, document registries, dispute mechanisms, consumer protection etc) does not yet exist. Legal frameworks in different jurisdictions vary in their recognition of e-commerce. Nonetheless, management needs to consider legal and regulatory issues related to the entity's e-commerce activities, for example, whether the entity has adequate mechanisms for recognition of taxation liabilities, particularly sales or value-added taxes, in various jurisdictions. Factors that may give rise to taxes on e-commerce transactions include the place where:

a. the entity is legally registered;

b. its physical operations are based;

c. its web server is located;

d. goods and services are supplied from; and

e. its customers are located or goods and services are delivered.

These may all be in different jurisdictions. This may give rise to a risk that taxes due on cross-jurisdictional transactions are not appropriately recognized.

23. Legal or regulatory issues that may be particularly relevant in an e-commerce environment include:

a. adherence to national and international privacy requirements;

b. adherence to national and international requirements for regulated industries;

c. the enforceability of contracts;

d. the legality of particular activities, for example Internet gambling;

e. the risk of money laundering; and

f. violation of intellectual property rights.

24. SAS 120 "Consideration of laws and regulations in an audit of financial statements" requires that when planning and performing audit procedures and in evaluating and reporting the results thereof, the auditors recognize that noncompliance by the entity with laws and regulations may materially affect the financial statements. SAS 120 also requires that, in order to plan the audit, the auditors should obtain a general understanding of the legal and regulatory framework applicable to the entity and the industry and how the entity is complying with that framework. That framework may, in the particular circumstances of the entity, include certain legal and regulatory issues related to its e-commerce activities. While SAS 120 recognizes that an audit cannot be expected to detect noncompliance with all laws and regulations, the auditors are specifically required to perform procedures to help identify instances of noncompliance with those laws and regulations where noncompliance should be considered when preparing financial statements. When a legal or regulatory issue arises that, in the auditors' judgment, may result in a material misstatement of the financial statements or have a significant effect on the auditors' procedures or the audit report, the auditors consider management's response to the issue. In some cases, the advice of a lawyer with particular expertise in e-commerce issues may be necessary when considering legal and regulatory issues arising from an entity's e-commerce activity.

Internal Control Considerations

25. Internal controls can be used to mitigate many of the risks associated with e-commerce activities. In accordance with SAS 300 "Audit risk assessments and accounting and internal control systems", the auditors consider the control environment and control procedures the entity has applied to its e-commerce activities to the extent they are relevant to the financial statement assertions. In some circumstances, for example when electronic commerce systems are highly automated, when transaction volumes are high, or when electronic evidence comprising the audit trail is not retained, the auditors may determine that it is not possible to reduce audit risk to an acceptably low level by using only substantive procedures. CAATs are often used in such circumstances (refer to PN 1009, "Computer-Assisted Audit Techniques").

26. As well as addressing security, transaction integrity and process alignment, as discussed below, the following aspects of internal control are particularly relevant when the entity engages in e-commerce:

a. maintaining the integrity of control procedures in the quickly changing e-commerce environment; and

b. ensuring access to relevant records for the entity's needs and for audit purposes.

Security

27. The entity's security infrastructure and related controls are a particularly important feature of its internal control system when external parties are able to access the entity's information system using a public network such as the Internet. Information is secure to the extent that the requirements for its authorization, authenticity, confidentiality, integrity, non-repudiation and availability have been satisfied.

28. The entity will ordinarily address security risks related to the recording and processing of e-commerce transactions through its security infrastructure and related controls. The security infrastructure and related controls may include an information security policy, an information security risk assessment, and standards, measures, practices, and procedures within which individual systems are introduced and maintained, including both physical measures and logical and other technical safeguards such as user identifiers, passwords and firewalls. To the extent they are relevant to the financial statement assertions the auditors consider such matters as:

    a. the effective use of firewalls and virus protection software to protect its systems from the introduction of unauthorized or harmful software, data or other material in electronic form,

    b. the effective use of encryption, including both:

        i. maintaining the privacy and security of transmissions through, for example, authorization of decryption keys; and

        ii. preventing the misuse of encryption technology through, for example, controlling and safeguarding private decryption keys;

    c. controls over the development and implementation of systems used to support e-commerce activities;

    d. whether security controls in place continue to be effective as new technologies that can be used to attack Internet security become available; and

    e. whether the control environment supports the control procedures implemented. For example, while some control procedures, such as digital certificate-based encryption systems, can be technically advanced, they may not be effective if they operate within an inadequate control environment.

Transaction Integrity

29. The auditors consider the completeness, accuracy, timeliness and authorization of information provided for recording and processing in the entity's financial records (transaction integrity). The nature and the level of sophistication of an entity's e-commerce activities influence the nature and extent of risks related to the recording and processing of e-commerce transactions.

30. Audit procedures regarding the integrity of information in the accounting system relating to e-commerce transactions are largely concerned with evaluating the reliability of the systems in use for capturing and processing such information. In a sophisticated system, the originating action, for example receipt of a customer order over the Internet, will automatically initiate all other steps in processing the transaction. Therefore, in contrast to audit procedures for traditional business activities, which ordinarily focus separately on control processes relating to each stage of transaction capture and processing, audit procedures for sophisticated e-commerce often focus on automated controls that relate to the integrity of transactions as they are captured and then immediately and automatically processed.

31. In an e-commerce environment, controls relating to transaction integrity are often designed to, for example:

    a. validate input;

    b. prevent duplication or omission of transactions;

c. ensure the terms of trade have been agreed before an order is processed, including delivery and credit terms, which may require, for example, that payment is obtained when an order is placed;

d. distinguish between customer browsing and orders placed, ensure a party to a transaction cannot later deny having agreed to specified terms (non-repudiation), and ensure transactions are with approved parties when appropriate;

e. prevent incomplete processing by ensuring all steps are completed and recorded (for example, for a business to consumer transaction: order accepted, payment received, goods/services delivered and accounting system updated) or if all steps are not completed and recorded, by rejecting the order;

f. ensure the proper distribution of transaction details across multiple systems in a network (for example, when data is collected centrally and is communicated to various resource managers to execute the transaction); and

g. ensure records are properly retained, backed-up and secured.

Process Alignment

32. Process alignment refers to the way various IT systems are integrated with one another and thus operate, in effect, as one system. In the e-commerce environment, it is important that transactions generated from an entity's web site are processed properly by the entity's internal systems, such as the accounting system, customer relationship management systems and inventory management systems (often known as "back office" systems). Many web sites are not automatically integrated with internal systems.

33. The way e-commerce transactions are captured and transferred to the entity's accounting system may affect such matters as:

a. the completeness and accuracy of transaction processing and information storage;

b. the timing of the recognition of sales revenues, purchases and other transactions; and

c. identification and recording of disputed transactions.

34. When it is relevant to the financial statement assertions, the auditors consider the controls governing the integration of e-commerce transactions with internal systems, and the controls over systems changes and data conversion to automate process alignment.

The Effect of Electronic Records on Audit Evidence

35. There may not be any paper records for e-commerce transactions, and electronic records may be more easily destroyed or altered than paper records without leaving evidence of such destruction or alteration. The auditors consider whether the entity's security of information policies, and security controls as implemented, are adequate to prevent unauthorized changes to the accounting system or records, or to systems that provide data to the accounting system.

36. The auditors may test automated controls, such as record integrity checks, electronic date stamps, digital signatures, and version controls when considering the integrity of electronic evidence. Depending on the auditors' assessment of these controls, the auditors may also consider the need to perform additional procedures such as confirming transaction details or account balances with third parties (refer to SAS 402 "External confirmations").

Compatibility with International Auditing Practice Statements

37. This Practice Note is, in all material respects, in accordance with International Auditing Practice Statement 1013 "Electronic Commerce – Effect on the Audit of Financial Statements".