The Impacts of Electronic Commerce on Auditing Practices: An Auditing Process Model for Evidence Collection and Validation

Chien-Chih Yu*, Hung-Chao Yu and
Chi-Chun Chou
National ChengChi University, Taiwan, ROC

ABSTRACT **The main purposes of this paper are twofold. First, the paper identifies and discusses the potential impacts of electronic commerce on auditing practices in the emerging paperless on-line transaction environment. Second, it provides two auditing process models that incorporate modern network security techniques and show how an audit can be conducted in an EC environment. A *periodical auditing process model* (PAPM) is proposed to demonstrate how secure electronic technologies can be used to facilitate the auditor's evidence collection and validation process for annual and semi-annual audits. We also present a *continuous auditing process model* (CAPM) which extends the functions of PAPM for continuous auditing. In CAPM, a real-time transaction monitoring system is used to link to firms' accounting information systems for assisting the auditor to detect abnormal activities and generate exception reports on a continuous basis. The CAPM approach intends not only to ensure integrity and effectiveness of the entire accounting system, but also to guarantee the correctness and usefulness of the constantly generated financial statements for public dissemination. The main contribution of this paper is that it illustrates a conceptual framework which shows the feasibility of continuously auditing electronic transactions in the EC environment. Copyright © 2000 John Wiley & Sons, Ltd.**

INTRODUCTION

During the past few years, the rapid advance of Internet technologies and World Wide Web (WWW) applications has significantly contributed to the development of electronic commerce (EC). EC integrates network technologies, information management, security service, and value-added networks (VANs) to provide on-line services such as product delivering, electronic shopping, home banking, and secured on-line payments.[1] Customers may

* Correspondence to: Chien-Chih Yu, Department of Management Information Systems, National Cheng Chi University, Taipei, Taiwan, ROC.
E-mail: ccyu@mis.nccu.edu.tw

[1] Some well-known EC examples include the Amazon BookStore, TravelWeb, FlowerShop, E*Trade, Internet Shopping Network (ISN), Security First Network Bank (SFNB), CUC International, Time

Received 10 September 1998
Revised 29 July 1999
Accepted 7 March 2000

International Journal of Intelligent Systems in Accounting, Finance & Management
Int. J. Intell. Sys. Acc. Fin. Mgmt. **9**, 195–216 (2000)

directly inquire and order merchandise from their own remote browsers and make payments through secured payment mechanisms. Companies can build their own homepages or Web sites to trade with other companies and individual customers world-wide without time and space constraints. Technically speaking, almost all business activities (e.g. sales, ordering, purchasing, and payment) can function well in an EC environment. Some specific types of products (e.g. computer software, network publications) can even be transmitted and exchanged in electronic format. Through the application of Internet technologies, the recording, authenticating, summarizing, and maintaining of transaction documents can be accomplished in the cyberspace, leading to electronically paperless transaction trails. Due to EC's potential importance and contribution to future success, companies across various business domains are now considering the challenges and opportunities of adopting EC to their business and management activities (Borenstein *et al.*, 1996; Camp and Sirbu, 1997; Graham, 1996; Kalakota and Whinston, 1996; Kogan *et al.*, 1996; Sivori, 1996; Tenenbaum *et al.*, 1997).

During the late 1970s and early 1980s, EC became widely spread within companies in the form of electronic data interchange (EDI). Related work in the literature focuses primarily on EDI's importance (Ansary, 1993; Meier, 1992), implementation issues (Bruce, 1990; Emmelhainz, 1993; Gunther, 1994), communication standards (Eckerson, 1991; Wheatman, 1991), audit and internal control issues (Chan, 1991; CICA, 1993, 1996; Hansen and Hill, 1989; Marcella *et al.*, 1992; Walden and Braganza, 1993), as well as security and legal issues (Chalmers, 1990; Jones, 1992; Wright, 1992), but seldom discusses whether the traditional audit process is still appropriate in EDI and how new security techniques can be incorporated (e.g. firewalls, data encryption methods, digital signature, and digital envelope) into an audit engagement.

In the 1990s, the advent of the WWW on the Internet represented a turning point in EC by providing an open and easy-to-use technology solution to the problem of information publishing and dissemination (Kalakota and Whinston, 1997). In contrast to EDI, which requires substantial hardware investment and specific intermediaries (i.e. standard formats and translation software), the Web not only facilitates business transactions through general WWW browsers, but also enables more diverse business activities to be conducted globally. The special characteristics of the Web (e.g. open environment, easy application setting, and low entry barrier) provide small and medium-sized enterprises with an opportunity to compete on a more equal technological footing with resource-rich multinational companies. Because WWW introduces a more complicated business environment than EDI, new control and auditing issues have to be identified and addressed in an EC environment. In the past few years, studies related to the implementation of EC to various business domains have increased substantially (Borenstein *et al.*, 1996; Camp and Sirbu, 1997; Kalakota and Whinston, 1996; Panurach, 1996; Piven, 1997; Pyle, 1996; Tenenbaum *et al.*, 1997). However, there is still a lack of discussion about the impacts of EC on firms' overall internal control procedures and how an audit can be conducted in an EC environment.

The success of EC depends heavily on consumers' trust and confidence on protection related to the legitimacy of online business, the privacy of personal information, and the security of business transactions. In fact, many studies indicate that only about 20–25% of the online users are willing to complete a transaction in the cyberspace.[2] In response to customers' concerns about the risk of trading electronically, the American Institute of Certified Public Accountants (AICPA) and the Canadian

Warner's Pathfinder, Wall Street Journal Interactive, and Disney On-line.

[2] In mid-1997, the AICPA commissioned Yankelovich Partners to conduct a survey of 1003 Americans who were 18 years old or older and who subscribed to on-line service. The results indicated that most of the subjects would not provide their income (91%), credit card number (85%), phone number (74%), and address (67%) when shopping on-line. Lack of security was the primary reason for subjects not buying products on-line.

Institute of Chartered Accountants (CICA) have recently issued a new guideline, the *WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce*, to ensure that an entity's Web site institutes effective controls and practices to protect consumer interests (AICPA and CICA, 1999a).[3] It should be noted that the *CPA WebTrust* only introduces a new assurance service opportunity to the public accounting profession, but provides few or no guidelines about whether traditional auditing procedures and standards are still appropriate to an EC audit engagement.

The primary goal and contribution of this paper are twofold. First, this study explores some possible impacts of EC on auditing practices. In particular, new audit risks and internal control considerations are identified and discussed. Second, it proposes two new auditing process models that incorporate modern network security techniques and show how a typical audit can be conducted in an EC environment. In the *periodical auditing process model* (PAPM), traditional annual and semi-annual audits are conducted using current secure electronic transaction technologies to facilitate the collection and validation of electronic audit evidence.[4] The *continuous auditing process model* (CAPM) extends the functions of PAPM using a real-time transaction monitoring system and predefined auditing rules to detect abnormal events and generate exception reports on a continuous basis. The CAPM aims at supporting safe accounting operations and allowing for timely dissemination of approved financial information and statements on companies' Web sites. It should be noted that these models are not new computer-assisted auditing techniques (CAATs), but may efficiently use the traditional CAATs in an EC environment.

The remainder of this paper is organized as follows. The next section discusses important impacts and potential problems of EC on auditing practices. New audit risks and internal controls are identified. The third section proposes a conceptual framework for EC auditing and introduces two EC auditing process models, the PAPM and the CAPM. A summary and conclusion is provided in the final section.

THE IMPACTS OF EC ON AUDITING PRACTICES

In a paperless EC environment, the need for physical paper evidence will significantly decrease. In addition, since most of the business transactions will be done and more timely financial statements will be requested and distributed through the Internet, companies have to design new accounting information systems which not only record and trace transaction information instantaneously, but also cross-check internal and external documents automatically. An even more important issue is the need to design new internal control procedures to ensure the integrity and authentication of EC transactions and protect the private key, digital signature, and the whole Web system together with related databases. These changes introduce new challenges to the auditing profession. In fact, EC is not, by itself, the driver of audit impacts. It is the new business practices driven by the EC that require the auditing profession to update its understanding of companies' new business processes, reassess audit risks, and determine how these may affect the overall audit.

This section discusses the impacts of EC on audit risk assessment and the design of internal controls. We focus on these two issues because of their relative importance in the overall audit process. As suggested in the AICPA (1983) *Statements of Auditing Standards* (SAS) No. 47, the audit risk concept should be used for planning purposes to decide how much evidence

[3] Three principles are specified in the guideline: the *business practices disclosure principle* (i.e. the entity discloses its EC business practices and executes transactions in accordance with its disclosed practices), the *transaction integrity principle* (i.e. the entity maintains effective controls to provide an assurance that customers' orders placed are completed and billed as agreed), and the *information protection principle* (i.e. the entity maintains effective controls to provide an assurance that private customer information obtained is protected).

[4] In Taiwan, both the semi-annual and annual financial statements should be audited. In the USA, however, only the annual financial statements should be audited.

to accumulate in each transaction cycle. SAS No. 78 further indicates that internal control is a process designed to provide reasonable assurance regarding the achievement of reliable financial reporting, effective and efficient operations, and compliance with laws and regulations. More important, the study of a firm's internal controls and the assessment of control risks are the major components in the audit risk model.

New Audit Risks in an EC Environment

When an EC-based system is adopted by a business entity, a number of new features affect the audit risk and its three components (i.e, inherent risk, control risk, and detection risk) in the following five respects.

Economic Interdependence

One of the main objectives of EC is to facilitate an entity's transactions and business decisions through the Internet with a large number of trading partners and individual customers. This increased closeness of trading relationship and virtual business integration (e.g. *a supply chain*) may affect the inherent and control risks in an audit because a potential corruption in one trading partner's EC system may adversely affect other partners and customers. Therefore, the auditor should at least consider the following items in assessing the audit risk:

(1) The economic interdependence between the audit client and its major vendors, customers or other related entities.
(2) The extent to which the client's internal control policies and procedures interact with those of other trading partners.
(3) The changes in the client's internal control policies and procedures due to new EC trading activities.
(4) The control risk associated with financial statement assertions which may be affected by economic interdependence.

Total Systems Dependence

As a business entity relies heavily on EC (and thus on the Web system and related technologies), the corruption of applications and undetected errors will become a crucial issue to the entity's success in EC. An undetected error in a cash payment application, for example, may adversely affect an entity's cash flows and its public confidence to customers and suppliers. In fact, total systems dependence can also cause substantial losses that, in turn, raise doubts as to whether there was a failure in the system (Rittenberg and Schwieger, 1997). Several issues should be taken into consideration when auditing an EC company:

(1) Errors in network processing and communication systems may result in the transmission of incorrect transaction information and the reporting of inaccurate information to management. If not detected in time, inaccurate and incomplete information may result in inappropriate decisions and potential business losses, leading to higher control risk.
(2) Since the success of EC relies on good internal controls built into the system, the auditor should be able to find effective and efficient internal control procedures that may reduce the control risk associated with management's assertions.

In light of the increasing importance of information systems to the success of business entities, the AICPA and the CICA have recently issued a new guideline, the *SysTrust Principles and Criteria for Systems Reliability*, to provide assurance that an entity's systems are designed and operated to generate reliable information.[5] In fact, this new service is part of a broader future goal to supply real-time assurance on databases and information systems. Since in an

[5] According to *SysTrust*, a reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. Four principles are suggested to evaluate the reliability of a system: *availability* (i.e. the system is available for operation and use at times set forth in service-level statements or agreements), *security* (i.e. the system is protected against unauthorized physical and logical access), *integrity* (i.e. system processing is complete, accurate, timely, and authorized), and *maintainability* (i.e. the system can be updated when required in a manner that continues to provide for system availability, security, and integrity).

EC environment business entities rely heavily on systems, *SysTrust* will contribute to the progress of EC as system assurance services become a reality (AICPA and CICA, 1999b).

Potential Loss of Transaction Trails and Data

In an EC environment, there will be less paper available for verifying and reconciling transactions. Much of the information generated from an entity's EC system will be in electronic form. The validity of the internal and external electronic evidence depends heavily on new security technologies and appropriate transaction protocols. Such a paperless environment may affect traditional audits in the following ways:

(1) Issues such as the validity of electronic evidence, the security of transferring electronic information, the control of network applications, and the standards and formats of electronic audit trails will dramatically affect the determination of detection risk.
(2) Policies for retention and recovery of transaction data are important. Without these controls, an entity may not be able to provide adequate and appropriate evidence for cost-efficient audits.
(3) Since the business cycle is compressed in an EC environment, many of the balance sheet accounts (e.g. inventory and accounts receivable) may be significantly reduced. This may have impacts on the inherent and control risks of these accounts.
(4) Similar to EDI, the implementation of EC may result in a reduction of accounting cycle periods between trading partners. Therefore, traditional control procedures such as a monthly accounts receivable statement prepared at the end of an accounting cycle may not be necessary because reconciliation can be performed through the Internet by product line, season, or other operating factors (CICA, 1996).
(5) Because individual customers can trade with an entity through the Internet, companies face an increase in transactions with small dollar amounts (e.g. the purchase of NBA star cards by teenagers). These and other *micro-payment* transactions may affect the inherent and control risks in accounts such as Cash and Sales.

Reliance on Third Parties

A business entity will rely more on other third parties such as the Internet service providers (ISP) to ensure that transactions are communicated and processed correctly and are not inappropriately disclosed.[6] Errors, security breaches, and processing disruptions in the third party's system or network may have adverse impacts on the entity's operations. Examples of such threats include the disclosure of confidential information, the entry of invalid or unauthorized transactions, the incomplete or delayed transmission of data, and the penetration of system and applications by viruses or hackers. Therefore, the auditor should at least consider the following issues in planning an audit:

(1) How the ISPs' control policies and procedures may affect the three risk components associated with the audit client's financial statement assertions.
(2) How the audit client's internal control policies and procedures may interact with those of the ISPs.
(3) The nature of services provided by the ISPs (i.e. whether services are highly standardized and used by many companies).
(4) The nature and sufficiency of auditable data owned by the audit client and the ISPs.
(5) The ISPs' capabilities and reputation (e.g. professional qualification, financial strength, competence, and integrity).

After considering the importance of ISPs to the success of EC, the AICPA and the CICA have recently issued the *WebTrust-ISP Principles and Criteria for Internet Service Providers in Electronic Commerce.* This guideline provides assurance to the customers that the ISPs would

[6] According to Kalakota and Whinston (1997), the ISPs offer a wide variety of technologies and services such as Internet access for customers and organizations (e.g. America Online), network management, system integration, and backbone access services (e.g. UUNET), client and server software for navigating and publishing material on the Internet (e.g. Netscape), and payment systems for online purchases (e.g. CyberCash).

follow a recognized set of principles in the conduct of its EC business and would assist their customers in obtaining a *WebTrust Business-to-Consumer Seal of assurance* for their Web sites (AICPA and CICA, 1999c).[7]

Loss of Confidentiality

In an EC environment, sensitive information may be accidentally or intentionally disclosed on the Web. In fact, a major security threat companies may encounter is the high exposure and availability of transaction applications on the Internet. Because of the high concentration of data controlled by a few individuals, the high speeds of computer processing systems, and the increased accessibility to data, it becomes much easier for external parties to observe or obtain an entity's information without its permission. For dealing with this situation, the auditor should at least consider the following items to assess the audit risk:

(1) The access control policies, processes, technologies, and security mechanisms adopted.
(2) The data encryption and decryption methods used.
(3) The intrusion prevention and detection functions applied.

New Internal Controls in an EC Environment

SAS No. 56 and *78* provide general guidelines for the internal control framework in an electronic data processing (EDP) environment.[8] There are three key components in this framework: the general controls, the application controls, and the on-line real-time controls. Even though most of these control components are still appropriate in the EC environment, special attention should also be paid to the following new control features.

Security Controls of Electronic Documents Transfer

Security controls ensure the integrity, confidentiality, privacy, authentication, and nonrepudiation of transaction information to avoid security threats such as illegal access, sniffing, eavesdropping, modification, repudiation and spoofing. Companies may need to carefully consider the following issues:

(1) How proper security control technologies (e.g. password, firewalls, data encryption, digital signature and digital envelope) can be tested and used.
(2) How appropriate secure electronic transaction protocols (e.g. the SET standard for Internet payment security, the S-HTTP and S/MIME protocols for application layer security, the SSL protocol for session layer security, and the AH and ESP protocols for network layer security) can be adopted.
(3) How certificate authorities (CA) should be chosen for ensuring secure electronic transactions and safe electronic document interchanges.

The communication control protocols and facilities should also include algorithms for predetermining whether noise or loss of signals has altered the content of messages during transmission and if so, automatically requesting

[7] The *WebTrust-ISP Principles and Criteria* specify three principles: the *business practices disclosure principle* (i.e. the ISP discloses its business practices for EC services and provides such services in accordance with its disclosed business practices), the *availability principle* (i.e. the ISP maintains effective controls to provide reasonable assurance that the customer's access to the ISP network access point and related EC services is available as disclosed by the ISP), and the *security and privacy principle* (i.e. the ISP maintains effective controls against unauthorized physical and electronic access to the ISP's EC operating systems and applications, and to private customer information obtained as a result of EC activities to provide reasonable assurance that access to systems and customer accounts is restricted to authorized individuals and that such private customer information is protected from uses not related to the entity's business).

[8] SAS No. 48, *The Effects of Computer Processing on the Audit of Financial Statements*, has been integrated within sections 311.03, 311.09–311.10, 318.07 (superseded by SAS No. 56), 320.33–320.34 (superseded by SAS No. 55), 320.37 (superseded by SAS No. 55), 320.57–320.58 (superseded by SAS No. 55), 320.65 – 320.68 (superseded by SAS No. 55), and 326.12. SAS No. 56 was later amended by SAS No. 78 to incorporate the new definitions and descriptions of internal controls specified in the COSO report.

message re-transmission or recovery. Table 1 summarizes some commonly used security control methods (Bhimani, 1996; Carroll, 1997; Cobb, 1996; Herringshaw, 1997).

Controls to Maintain Transaction Trails

Since the transaction trails will change from physical documents to electronic format, a business entity should concentrate more on the separation of duties and authorization and should develop computer applications to record and maintain these transaction trails for supporting nonrepudiation and future cross-checking. In general, effective procedures of controlling and maintaining transaction trails include the following:

(1) Create and design transaction logs in appropriate format to record processed and failed transactions, buyer–seller acknowledgments, and time sequence of processing. These log files provide evidence that transactions are recorded in the correct accounting period (through the use of electronic time stamps). Acknowledgments between buyers and sellers can ensure that transactions are recorded on a timely basis and transactions messages are understood by both parties, are genuine, and have not been altered.
(2) Use batch control totals when transactions are initiated or received and develop dual recording or parallel monitoring system to ensure the completeness and accuracy of transaction trails.

Table 1 Commonly used security methods for electronic transactions

Security requirements	Security threats	Security methods
Integrity	Illegal modification, data missing, replacement, deletion, destruction	Serial number control, time stamp, MAC code, digital signature
Authentication	Transaction spoofing	User ID, password, digital signature
Non-repudiation	Denial of message spending or transaction making	Digital signature
Confidentiality	Eavesdropping, illegal monitoring, sniffing	Data-encryption methods, digital envelope
Access control	Illegal user access, misuse of data	Qualified systems and software, user ID, password, firewall, intrusion detection system

Security Controls of Electronic Signatures

Being different from the password, which is often used to prevent illegal access to private information, an electronic signature serves not only as a means of ensuring the validity of transaction trails, but also as a proof of transaction between seller and buyer. Because of its importance to business transactions, public and private keys for electronic signature should be safeguarded in a way that is different from that of general assets. More specifically, safeguarding of private keys should be part of the overall approval and authentication process because private keys should only be used to digitally sign a document or open a digital envelope when a transaction has been approved or authenticated. Therefore, based on the principle of separation of duties, the safeguarding of private keys should be independent of the recording and executing of transactions. In general, the responsibilities of key management can be divided in the following ways:

(1) The managers in charge of transaction approvals should be responsible for safeguarding private keys.
(2) The managers in charge of transaction executions should be responsible for safeguarding encryption and decryption algorithms.

It should be noted that the protection of public keys and its registration profiles depends on the feasible hierarchical structure set by the certificate authorities.

Security Controls of Application Programs and Software

As mentioned above, a major security threat many companies may encounter is the high exposure and availability of transaction applications on the Internet. To overcome this problem, companies may adopt control techniques such as firewall or other end-to-end controls to avoid inappropriate execution or destruction of these application programs and software. In addition to these access control problems, more and more application providers either use the Java applets or other external programs with a common gateway interface (CGI) to execute or activate database retrieval or other computation processes across different application platforms. In fact, verifying application programs and software will become a major part of the auditor's overall auditing process. Some security techniques for controlling mobile codes or webwares include firewalling and code signing (Fellen, 1997; Rubin and Geer, 1998). In general, the key control procedures in a company's transaction processing system and management information system should include:

(1) Software/hardware controls, network management controls, and database access controls.
(2) Firewalls set up, virus check.
(3) The examination of applications and software distributed on the Internet.

Controls of Internet Service Providers

Control procedures adopted by the ISPs should also be considered to ascertain that sufficient and valid transaction security and integrity exist. Most ISPs may provide automatic controls in the recovery of damaged data, protection against data loss, and error-checking. Depending on the extent of services provided by the ISPs, two considerations may be taken into account:

(1) The auditor may wish to consider obtaining a report from a third-party specialist ensuring the adequacy and validity of network controls on the ISP's system.
(2) The auditor should also pay attention to issues such as the ISP's continuing service in case of disaster and the provision of confidentiality.

Earlier Preventive Control Points

In an EC environment, *preventive* controls as well as traditional *detection* controls should be embedded in transaction processing systems. This is analogous to the progress in total quality management, where quality assurance based on inspection and rework has been largely replaced by the redesign of processes and products to eliminate the sources of defects (Elliott, 1995). More importantly, EC causes the control points to occur earlier than before. In a merchandising company, for example, controls over payments of accounts payable should be accomplished by automatically reconciling the vendor's invoices with vouchers generated by the company's acquisition systems. The company then pays based on the trading partner agreements that have been built into the computer applications which, in turn, automatically attach a 'PAID' mark to the vouchers. In this example, it would be inefficient for the company to use *ex post* detection controls such as manually calculating the extensions on the vendor invoices to determine whether the prices are correct. It should be noted that, for companies to be successful in an EC environment, preventive controls should be considered during the analysis and design stage of developing EC applications.

Other Issues of EC Impacts on Overall Audit Process

While audit risk and internal controls are important components in the overall audit process, there are other issues that deserve the public accounting profession's attention. Table 2 provides a valuable reference for auditors to identify some possible impacts of EC on each stage of the audit process. It should be noted that the study of the interactions between EC and auditing is still at an infant stage. In fact, most of the issues proposed on Table 2 are new concepts and ideas. Therefore, more effort should be devoted by the profession and academics of auditing and information technology domains to provide some satisfactory solutions.

Table 2. Possible impacts of EC on the overall auditing process

Stages in auditing process	EC's possible impacts
Acceptance/continuance of clients	● What additional factors should be considered in determining the acceptance or continuance of clients? (e.g. Does the potential client provide real-time financial information on its Web site?) ● Where do we obtain information about these additional factors?
Audit planning	● How do we assess the materiality at both the individual account level and the overall financial statement level? ● Is there any new audit risk in an EC environment? Is the traditional audit risk model still appropriate? ● Are the traditional audit programs still appropriate? How do we modify them?
Understanding of client's ICS	● What are the key control points in an EC environment? How do we evaluate them? ● How do we obtain an understanding of a client's ICS and make a preliminary control risk assessment? ● What constitutes 'material weakness' in the client's ICS?
Tests of controls	● How do we test specific control points in the client's ICS (e.g. client's secure transaction mechanisms)? ● How do we determine the extent, nature, and timing of substantive tests? (e.g. If the control risk is assessed at the minimum level, is it still necessary to conduct substantive tests?)
Substantive tests of transactions and balances	● How do we verify the validity and authentication of the client's electronic evidence? ● Are the traditional five management assertions still appropriate in an EC environment? (e.g. How do we verify the existence of inventory of a on-line publishing company?) Is there any new assertion to be tested in an EC environment? ● What new audit technologies or procedures should the auditor use to test transactions and account balances?
Completion of audit field work	● How do we determine the sufficiency and competence of audit evidence? ● How do we evaluate the client's going concern in an EC environment? ● How do we detect related-party transactions in an EC environment?
Issuance of audit report	● Should the auditor express an opinion on the validity of the client's EC systems? ● Should the content of the audit report change to accommodate the client's use of EC operations?
Overall audit process	● Is the traditional audit process still appropriate? Are there any (new) stages which should be eliminated (incorporated)? ● What is the auditor's legal liability in an EC environment? (e.g. Should the auditor be responsible for the validity of the client's EC systems?) ● Are the formats and types of traditional working papers still apropriate?

AUDITING PROCESS MODELS IN THE EC ENVIRONMENT

During a financial statement audit in an EC environment, the auditor faces the problem of obtaining electronic transaction trails with digital signatures from more diffused sources (e.g. a remote download in a client–server architecture). In light of the transmission and authentication of electronic transactions and the demand for timely financial reporting, it is necessary to develop a new auditing process model as a guideline for the auditing profession. Based on the time interval of audits, two EC auditing process models are proposed: The *periodical auditing process model* (PAPM) and the *continuous auditing process model* (CAPM). The basic frameworks of these two models, together with real examples, are discussed in detail below.

The Periodical Auditing Process Model (PAPM)

To facilitate our discussion, a vendor invoice example is provided. The participants in this example include a *certificate authority* (CA), a *vendor* (*seller*) who sells goods and sends the invoice to a *buyer*, and the buyer's *auditor*. Figures 1 and 2 demonstrate the overall framework of this example.[9] This example has two distinct features. First, it shows how Internet security techniques can be used to maintain the credibility of electronic transaction evidence in an EC environment. Second, it does highlight some of the key EC control procedures for all entities and departments involved (to be discussed later). Due to the limitation of scope of the example, it is impossible to incorporate all internal controls detailed in the previous section. However, with appropriate modifications to the participants (i.e. CA, vendor, and buyer), this proposed framework can also be applied to other transaction cycles.

The Activities of the Certificate Authority

In Taiwan, the CA of vendor invoices is the Department of Treasury (DOT). In our vendor invoice example, the major activities of the CA include the following:

(1) **Authentication of Vendor Identity**: The DOT is responsible for the authentication of vendor identities, the approval and issuance of public key certificates for digital signature, and the maintenance of the vendor's public key in the public database. Generally, these tasks can also be carried out by other qualified authority organizations.

(2) **Approval of Applications of Vendor Invoices**: When a registered seller applies blank vendor invoices and invoice serial numbers from the DOT, a DOT agent should review the strength of the vendor's internal controls and decide whether to approve the application. Two criteria are important in this approval process:

- The auto-numbering control on the invoice-generating system: To ensure unique issuance of each blank invoice, the DOT has to incorporate an auto-numbering mechanism on its invoice-generating system to prevent blank invoices from duplicate usage by the vendor.
- The time stamp control on the invoice-issuance system: To maintain the validity of blank invoices for future use, the DOT must set up an automatic time stamp mechanism on its invoice-issuance system to ensure that no invoices can be used after a specific expiration date. This control procedure can also avoid the vendor's repeated use of the same invoice number.

(3) **Issuance of Prenumbered Blank Invoices**: After the approval of the invoice application, the DOT will first use the MD5 method to encrypt the approved blank invoices together with the serial numbers and expiry date into a message digest, and then use its private key to encrypt the message digest into a digital signature #1. Finally, the DOT will use the vendor's public key to encrypt both digital signature #1 and *original* invoice messages (i.e. the blank invoices, the serial numbers, and expiry date) into a digital envelope #1 and send it to the vendor. The upper-left part of Figure 1 demonstrates this process.

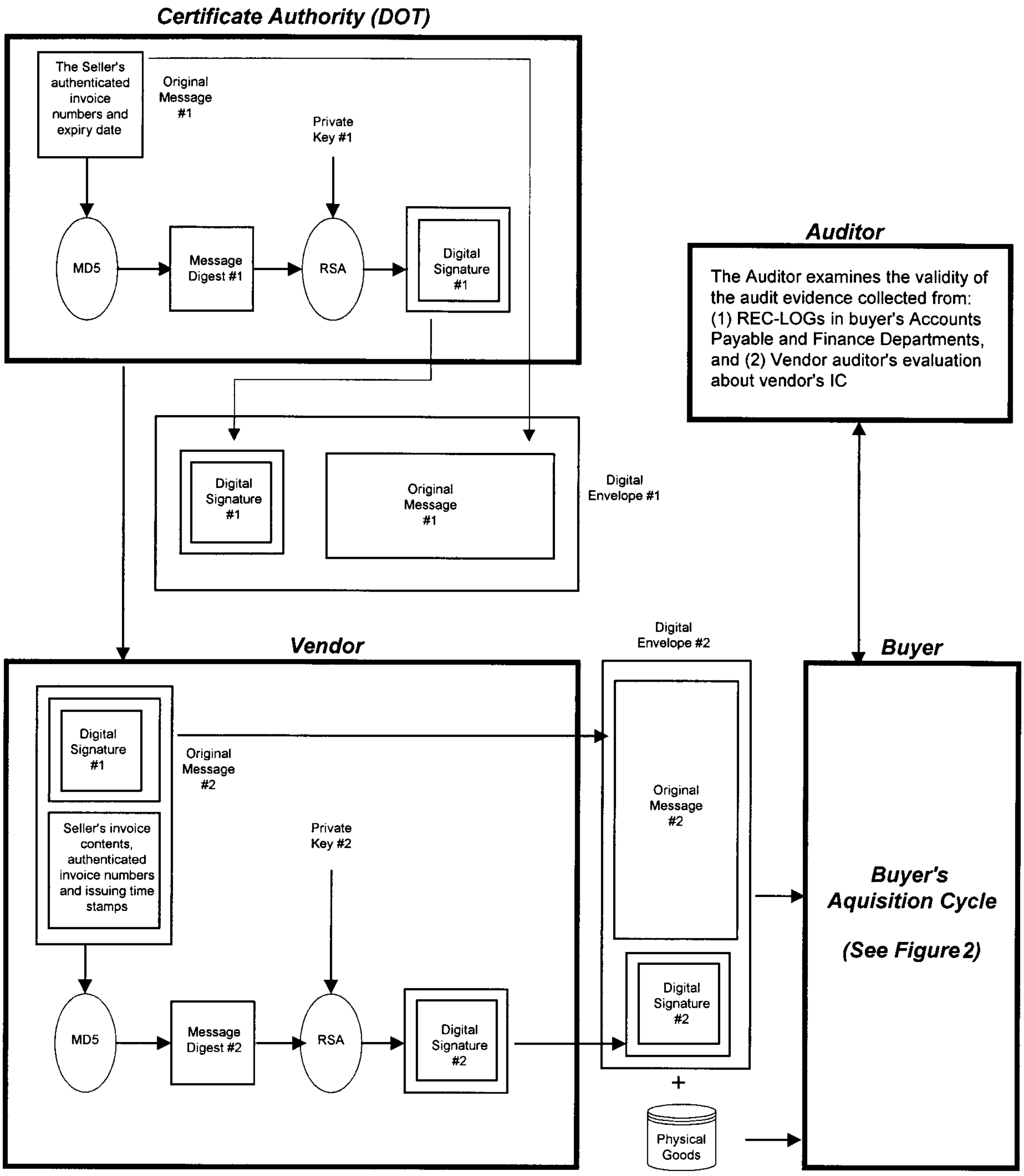
The Activities of the Vendor

In our invoice example, the vendor has the following two major activities:

(1) **Authentication of Blank Invoices**: The vendor uses a private key to open the digital envelope #1 received from DOT, and then uses the DOT's public key to verify the validity of digital signature #1 on the blank invoices.

(2) **Transmission of Invoices to the Buyer**:

[9] In current auditing practice, node 13 of Figure 2 should include a sequence of actions: return the goods to the vendor, notify the purchasing department to contact the vendor for an explanation, inform the accounts payable department for a debit memo, and record the returned goods on the return log file. However, incorporating all these actions may complicate Figure 2. Because the main purpose of Figure 2 is to demonstrate how the key internal control procedures discussed above can be implemented in the acquisition cycle, the term 'Disagreement Handling' was used to represent the whole sequence of actions.



MD5 = An encryption method that translates the initial message into message digest
RSA = A public key encryption algorithm invented by Rivest, Shamir, and Adleman.

Figure 1 The Vendor Invoice example.

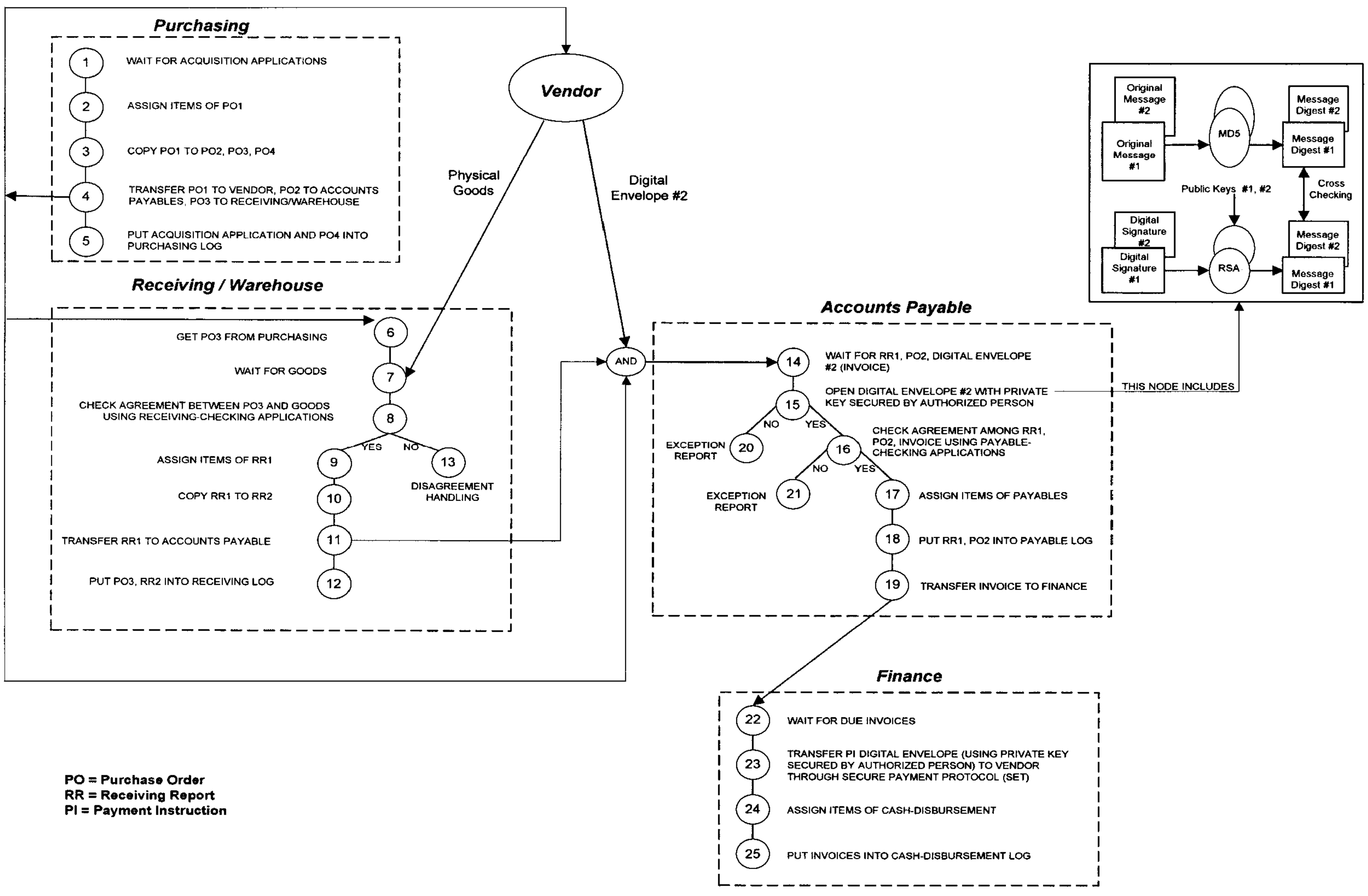

Purchasing
1 WAIT FOR ACQUISITION APPLICATIONS
2 ASSIGN ITEMS OF PO1
3 COPY PO1 TO PO2, PO3, PO4
4 TRANSFER PO1 TO VENDOR, PO2 TO ACCOUNTS PAYABLES, PO3 TO RECEIVING/WAREHOUSE
5 PUT ACQUISITION APPLICATION AND PO4 INTO PURCHASING LOG
Receiving / Warehouse
6 GET PO3 FROM PURCHASING
7 WAIT FOR GOODS
8 CHECK AGREEMENT BETWEEN PO3 AND GOODS USING RECEIVING-CHECKING APPLICATIONS
YES
NO
9 ASSIGN ITEMS OF RR1
10 COPY RR1 TO RR2
11 TRANSFER RR1 TO ACCOUNTS PAYABLE
12 PUT PO3, RR2 INTO RECEIVING LOG
13 DISAGREEMENT HANDLING
Vendor
Physical Goods
Digital Envelope #2
AND
Accounts Payable
14 WAIT FOR RR1, PO2, DIGITAL ENVELOPE #2 (INVOICE)
15 OPEN DIGITAL ENVELOPE #2 WITH PRIVATE KEY SECURED BY AUTHORIZED PERSON
NO
YES
20 EXCEPTION REPORT
16 CHECK AGREEMENT AMONG RR1, PO2, INVOICE USING PAYABLE-CHECKING APPLICATIONS
NO
YES
21 EXCEPTION REPORT
17 ASSIGN ITEMS OF PAYABLES
18 PUT RR1, PO2 INTO PAYABLE LOG
19 TRANSFER INVOICE TO FINANCE
THIS NODE INCLUDES
Original Message #2
Original Message #1
MD5
Message Digest #2
Message Digest #1
Public Keys #1, #2
Cross Checking
Digital Signature #2
Digital Signature #1
RSA
Message Digest #2
Message Digest #1
Finance
22 WAIT FOR DUE INVOICES
23 TRANSFER PI DIGITAL ENVELOPE (USING PRIVATE KEY SECURED BY AUTHORIZED PERSON) TO VENDOR THROUGH SECURE PAYMENT PROTOCOL (SET)
24 ASSIGN ITEMS OF CASH-DISBURSEMENT
25 PUT INVOICES INTO CASH-DISBURSEMENT LOG
PO = Purchase Order
RR = Receiving Report
PI = Payment Instruction

Figure 2 The buyer's internal controls and evidence validation process in an EC environment — acquisition cycle

Based on the time sequence of transactions, the vendor uses his invoice-preparation application (which may has auto-numbering and time stamp functions) to facilitate the recording of original transaction messages #2 (e.g. the goods sold, quantity, unit price, total price, and extensions) on the blank invoice. Finally, the vendor will use his private key to encrypt the original invoice messages #1, the original transaction messages #2, the DOT's digital signature #1, and the vendor's digital signature #2 into a digital envelope #2 and send it to the buyer. The lower-left part of Figure 1 demonstrates this process.

The Activities of the Buyer

To clearly describe how the auditor may conduct an audit in an EC environment, the *internal control description language* (ICDL) developed by Bailey *et al.* (1985) is used to create Figure 2.[10] Three points related to Figure 2 are worth mentioning. First, Figure 2 incorporates several key EC control procedures (as mentioned above) over input, process, and output of all departments involved in the buyer's acquisition cycle. Second, the ICDL is not the only tool for describing internal controls. Other advanced modeling tools (e.g. the unified modeling language, UML) can also be used to present the overall internal control structure. Finally, to focus mainly on EC auditing problems, we assume that the best practice of internal controls is already known by the auditor. However, if more internal control knowledge needs to be acquired through expert systems, an intelligent internal control analysis module such as the one proposed by Meservy *et al.* (1986) can be included in this model.

In our invoice example, two buyer's activities listed below are of major interest:

(1) **Authentication of Vendor's Invoice** (node 15): The buyer uses his private key to open digital envelope #2 and conducts two verifications. First, the buyer uses DOT's public key #1 to verify the validity of the vendor's invoice. The buyer then uses the vendor's public key #2 to verify the integrity and accuracy of the contents in the invoice. In Figure 2, this process is illustrated by the upper-right box of node 15.

(2) **Maintenance of Vendor's Invoice** (node 18): Based on the time sequence of transactions, the buyer uses his accounting applications (which may also has auto-numbering and time stamp functions) to record the content of original transaction messages #2 into its accounts payable database and logs. The payable log file and digital envelope #2 are maintained for future auditing.

Two comments regarding the buyer's internal documents should be made. First, the reliability of internal electronic documents depends heavily on the strength of the buyer's EC internal control structures. Because all internal documents are generated by the buyer's employees, their reliability will inevitably be lower than that of the external documents (e.g. vendor's invoice). Since in a highly-computerized company almost all internal documents are in electronic form and can be compared and cross-checked through system applications, the impacts of EC on internal audit evidence should not be as large as those on the external evidence. Second, the generation and management of internal electronic documents can be protected through the use of authentication and authorization control mechanisms to restrict

[10] According to Bailey *et al.* (1985), the ICDL was designed to support the description specifications of accounting internal controls. The ICDL consists of four parts: *agents* (i.e. actors in an information system), *objects* (i.e. things such as forms and records that are manipulated by the information system), *repositories* (i.e. storage facilities such as files for objects), and *commands* (i.e. models of tasks to be performed by agents). To encode the internal control representation, the *precedent constraint* (PC) concept is used. A sequential number is first assigned to each operation node, and precedent constraints for a given node are all nodes logically above the given node. For example, in Figure 2, node 24 represents the Finance department's preparation of a cash disbursement record. Tracing backwards through the model, all operations from node 1 to node 23 (including purchasing, receiving, bookkeeping of liability, and transferring of money to vendor) should be accomplished before recognizing cash disbursement. See Bailey *et al.* (1985) for more detailed discussions about the ICDL.

employees' access to system applications. Therefore, no public key or private key is necessary. In fact, many Intranet software providers have now incorporated the digital signature function into their packages (e.g. Netscape and Lotus). The combination of electronic documents and digital signature may provide a new way of secure authentication for internal documents.

The Activities of the Auditor

In auditing the buyer's acquisition cycle, the auditor *periodically* collects three types of evidence:

(1) **Buyer's transaction log files from the Purchasing, Receiving, Accounts Payable, and Finance departments** (corresponding to nodes 5, 12, 18, and 25, respectively). The auditor may use his own audit applications or softwares to cross-check the agreements among these log files to see if any exception exists. An exception report can be prepared for further examination.

(2) **Vendor's digital envelope #2 received by the buyer**. The auditor should (a) examine the validity and authentication of the original invoice messages #1, the original transaction messages #2, the DOT's digital signature #1, the vendor's digital signature #2, and the identity of the vendor, and (b) verify the integrity and accuracy of the contents in the invoice.

(3) **Internal control evaluations from Vendor's auditor**. Because errors, security breaches, and processing disruptions in the vendor's systems may adversely affect the validity of inputs to the buyer's operation systems, the buyer's auditor should review the vendor auditor's evaluation about the vendor's control policies and procedures related to his revenue cycle. The main purpose of doing this is to make sure that adequate controls have been established by the vendor to prevent errors, frauds, and illegal acts.

The Continuous Auditing Process Model (CAPM)

In a traditional financial statement audit, the auditor's responsibilities focus mainly on periodically collecting and assessing audit evidence, evaluating the strength of internal controls, and formulating an opinion on the fairness of financial statements. Therefore, there is no need for auditors to perform real-time monitoring operations. In the EC environment, however, due to the rapid advances in Internet technologies and the increased demand by the public for real-time electronic access to corporate databases, many public companies (e.g. AT&T, Microsoft, IBM) have already released their financial and operating information on their Web sites. In fact, there is strong evidence to believe that more and more public companies will post their key financial information on the Internet in the near future.[11] The requirement for correct and timely financial information leads to the need for quality audit service from the auditor to support continuous verification and dissemination of accounting information.[12] This brings new challenges to the public accounting profession: companies and the public need the auditor's report to accompany the financial information released on the Internet. Since in future we will be facing real-time business reporting with real-time auditing (Elliott, 1995), it is important for the auditing profession and the related academic to explore, in advance, how real-time auditing can be implemented to fulfil the statement-users' needs.[13]

[11] Liu et al. (1997) surveys the *Fortune 500* companies' Web sites and homepages and finds that 93.2% of the companies display their products and services and 86.1% of them provide company overview. About 79.3% of the companies present interactive feedback and 71.1% of them show 'what is new'.

[12] Currently, a special task force of the *Auditing Standards Board* (ASB) is surveying CPAs on their experience and beliefs relating to appropriate auditor responsibility when a client's financial statements are disseminated electronically, particularly on a Web site. See Pany (1998) for more details about this survey.

[13] Currently, an AICPA committee is preparing for a world in which all company data may be instantly accessible through a second generation of the Internet and virtually all businesses will interact electronically with the suppliers and customers. Essentially, the committee is planning for audits on a continuous basis in order to provide assurance about the data contained in that system (Rittenberg and Schwieger, 1997). Recently, a task force, sponsored

In response to the market's demand for timely and reliable information, the AICPA and CICA have just completed a research report, *Continuous Auditing*, to address the significant issues auditors will encounter in performing this type of service (AICPA and CICA, 1999d). Although this research report has described the continuous audit framework in various aspects (e.g. the nature, purpose, scope, and conditions for a continuous audit) and has identified significant matters auditors should consider (e.g. planning a continuous audit, collecting and evaluating evidence continuously, and reporting), there is still a lack of discussion on how to apply modern Internet techniques to facilitate the implementation of continuous auditing.[14] In this section, we propose a technically feasible continuous auditing process model (CAPM) that accommodates the spirit of real-time and continuous auditing in an EC environment.

The CAPM extends the PAPM and adopts the concept of a *continuous process auditing system* for internal auditing (Halper *et al.*, 1992; Kogan *et al.*, 1996; Vasarhelyi *et al.*, 1991) to meet the functional requirements of the external continuous auditing process. The CAPM system architecture and its whole environment are shown in Figure 3.

The overall CAPM operates in a client–server environment which contains two major components: the auditor's *continuous auditing process system* (CAPS) and the client's AIS on the Intranet and WWW server on the Internet. The client's AIS manages accounting information and generates financial reports. Three features of the CAPM are worth noting. First, the client's internal control procedures over the acquisition cycle, as depicted in Figure 2, are still appropriate for the CAPM. This is because the CAPM differs from the PAPM only in the way and frequency the auditor conducts an audit. Second, to perform real-time monitoring and auditing tasks, the CAPS is set up at the auditor's site and is connected to the client's AIS. The client's WWW server linking to its AIS provides retrieval and delivery services of financial information to the public. Finally, as will be discussed later, the CAPM architecture illustrates how the auditor may conduct a *system audit* and how the company may disseminate real-time and credible financial information on its Web site.

There are three layers in the auditor's CAPS: the data-capturing layer, the data-analysis layer, and the data-presentation layer. Each layer is discussed in detail below.

The Data-capturing Layer

This layer provides a bridge between the client's AIS and the auditor's CAPS which contains a data-capture function.

(1) **The Client's AIS**: The AIS consists of a report-generation function, a memory buffer, and a gateway to the CAPS. On a continuous basis, the client's AIS generates and stores financial reports (such as the receiving report, perpetual inventory summary, and cash payment summary in our vendor invoice example) and transaction log files (e.g. purchasing log, receiving log, payable log, and cash-disbursement log) in the memory buffer. The AIS's gateway device retrieves the reports and transaction log files from the memory buffer, adds digital signatures using the client's private key, puts them into a digital envelope using the auditor's public key, and then stores the encrypted envelope for the auditor's CAPS to capture or sends it to the CAPS directly. It also provides firewall and virtual private networking services to perform access control for preventing intrusion and maintaining audit trails as well as to facilitate the connection of CAPS to the corporate Intranet.

(2) **The Data Collector and Capturer**: The data capturer captures, on a continuous basis, the client's encrypted digital envelope using data-capturing facilities, opens the envelope

by the AICPA and the CICA, has finished a draft on continuous auditing issues. A new auditing standard, SAS No. 82 (*Considerations of Fraud in a Financial Statement Audit*), also calls for a continuous type of auditing to assist the auditor in preventing and detecting fraud (Landsittel and Bedard, 1997).

[14] Kogan *et al.* (1999) provide a historical and institutional background about the continuous online auditing (COA) and lists a series of research issues related to COA.

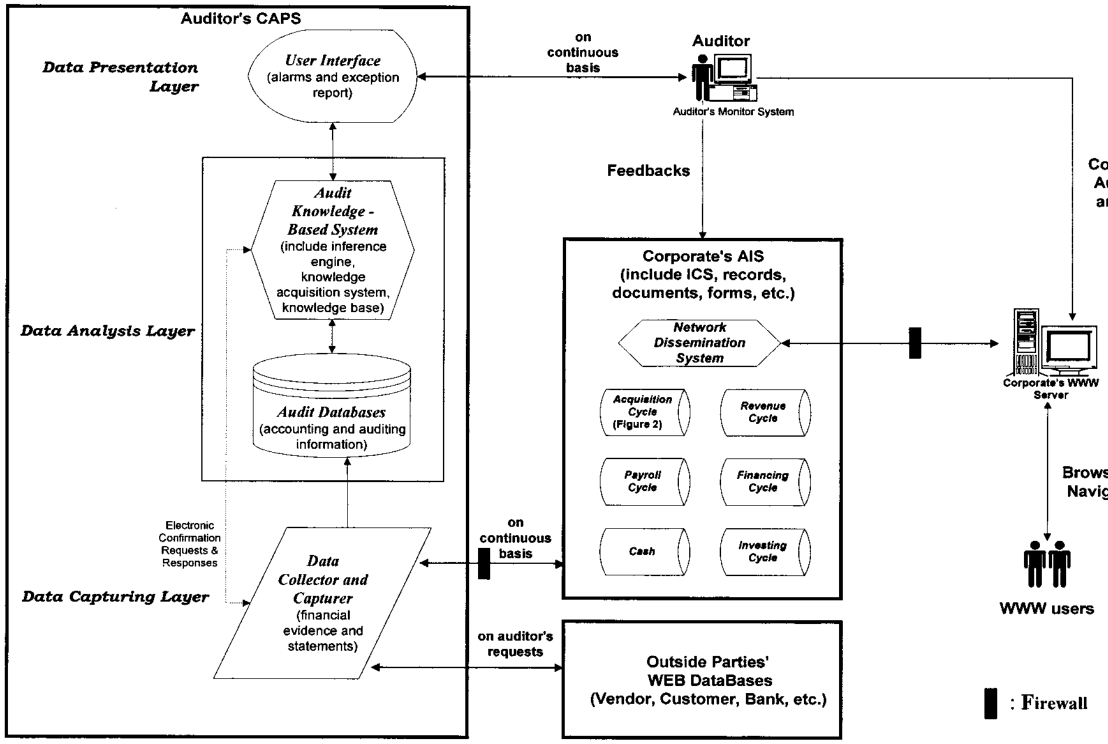

Auditor's CAPS
Data Presentation Layer
User Interface (alarms and exception report)
Audit Knowledge - Based System (include inference engine, knowledge acquisition system, knowledge base)
Data Analysis Layer
Audit Databases (accounting and auditing information)
Electronic Confirmation Requests & Responses
Data Capturing Layer
Data Collector and Capturer (financial evidence and statements)
on continuous basis
Auditor
Auditor's Monitor System
Feedbacks
Continuous Audit Seal and Audit Report
Corporate's AIS (include ICS, records, documents, forms, etc.)
Network Dissemination System
Acquisition Cycle (Figure 2)
Revenue Cycle
Payroll Cycle
Financing Cycle
Cash
Investing Cycle
on continuous basis
on auditor's requests
Outside Parties' WEB DataBases (Vendor, Customer, Bank, etc.)
Corporate's WWW Server
Browse and Navigation
WWW users
: Firewall

Figure 3 The CAPM architecture and system environment

using the auditor's private key, and checks the digital signatures using the client's public key. The original messages in the envelope (including the financial reports and the associated transaction log files) will then be stored in the audit database in the data-analysis layer for examinations. Since the financial reports and their associated log files are the main inputs to the CAPS, the system's capturing mechanism has to implement input controls to make sure that: (a) the received data are from the right client, (b) the received data are not modified or illegally accessed during network transmission, and (c) the client cannot repudiate the data transmitted. The data collector collects relevant information and documents from outside parties when further examination is needed.

The Data-analysis Layer

This layer consists of an audit database and an audit knowledge-based system for supporting verification and analysis of financial reports. Once the validity and authentication of the client's digital envelope in the data-capturing layer has been verified, specific fields of the financial reports and transaction log files are identified and automatically read into the *audit database*. Because these retrieved data will be examined and analyzed using the knowledge-based system and exception report and alarms will be generated accordingly when abnormal activities occur, the data-analysis layer should adopt certain control procedures to ensure that (a) the transactions comprising the financial reports and transaction logs are complete, and (b) no modification has been made to transactions that have been previously audited. At least two control procedures are helpful to fulfil these goals. First, all transactions that have been previously audited are marked to ensure that only those that have not been previously examined need to be examined. Only the unmarked transactions will be transferred to the audit database for further examination. This procedure also facilitates the cutoff tests of transactions and account balances because the first unmarked transactions in the log files should belong to the period under audit and the last marked transactions should belong to the previous audit period. Second, all transaction log files read into the audit database should be compared with the historical transaction logs already stored in the audit database since the last audit (these logs can be regarded as the electronic audit working paper). A 'difference report' listing differences in the marked transactions should be generated and sent to the knowledge-based system for further examination of potential fraud. If the client's AIS provides a function of generating update logs that summarizes all modifications to the client's audited (or marked) transaction log files, these update logs should also be retrieved and stored in the audit database to be compared with the auditor's 'difference report'. Any disagreement between the client's update logs and the auditor's 'difference report' may provide strong evidence about the effectiveness of client's internal controls in detecting unauthorized or illegal modifications to transaction master files.

The *audit knowledge-based system* and its associated knowledge base are the core in the CAPS. To support all fundamental analyses, diagnoses, verifications, and exception reporting for a typical acquisition cycle, the knowledge base and associated audit database should at least include the following:

(1) **All applicable GAAP and auditing rules**: These rules are used to link accounting metrics to standards for measurement and evaluation. For example, measurement and recognition criteria for inventory, accounts payable, and various expenses, level of indicators, warning messages for evaluating the system operation, and cutoff tests of accounts payable are included as predefined rules. The extracted data are analyzed and evaluated using these current GAAP and auditing standards for checking appropriateness and accuracy. In the vendor invoice example, some typical auditing rules may appear as:

Rule #1: IF VENDOR_STATUS = "related-party" AND ACCOUNTS_PAYABLE > $15,000
THEN VENDOR_ALARM = "active",

Rule #2: IF CASH_PAYMENT > $10,000 AND DUPLICATE_CHECK <> "paid"
THEN DUPLICATE_ALARM = "active",

Rule #3: IF (INVENTORY_TURNOVER – 5_YEAR_AVG) < 0.05*(5_YEAR_AVG)
THEN OBSOLETE_ALARM = "active",

Rule #4: IF ACCOUNTS_PAYABLE > $5,000 OR PAY_PAST_DUE_DAYS > 30
THEN OUTPUT "Vendor:", VENDOR, "account payable:", ACCOUNTS_PAYABLE, "days past due:", PAY_PAST_DUE_DAYS.

(2) **Auditor's preliminary assessments of risks**: The knowledge-based system will revise the auditor's preliminary assessments of the overall audit risk, inherent risk, and control risk periodically or continuously based on the evaluation results from previous audits.

(3) **Descriptions of the best acquisition practices**: The best acquisition practices in the client's industry as well as internal control structures (e.g. authorized requisition for goods, authorized purchase of goods according to company policies, receipt of goods, approval of items for payments, and cash disbursements) are described in a structured way. Using the ICDL, for example, Figure 2 can be stored in the audit database and compared with the best practices to detect substantial weaknesses in the design of client's internal controls. To facilitate a system audit on a continuous basis, the knowledge-based system is also structured to evaluate the effectiveness of the client's internal controls. To test whether the client can effectively prevent duplicate payments, for example, the knowledge-

based system may randomly select samples from the cash disbursement log and check whether each selected payment is accompanied by a 'PAID' seal or code. The sample deviation rate will then be compared with the predetermined tolerable deviation rate or achieved upper limit to revise the preliminary control risk assessment which, in turn, determines the detection risk.

(4) **Authorized vendor list and client's related parties**: The knowledge-based system selects purchase transactions and accounts payable balances to verify (a) whether the selected vendors are on the authorized vendor list, (b) whether any selected vendor is a related-party to the client, and (c) whether the account balances are correct. The knowledge-based system could randomly or judgmentally select account balances which meet specific criteria (e.g. all accounts payable balances in excess of $5000) and automatically send electronic confirmations to those vendors selected with an inquiry about the correctness of the account balances. It should be noted that the requests of electronic confirmation and vendors' responses are transmitted through the data-capturing layer, as depicted in Figure 3, by the dotted line connecting the knowledge-based system and the data collector and capturer. The knowledge-based system automates much of the selection process and monitors the correctness of vendor accounts continuously, rather than at the end of the year.

(5) **Analytical review applications and historical data**: To locate a potential misstatement or to address the completeness in the client's inventory account, for example, the knowledge-based system can compare the inventory turnover during the audit period with the industry and the client's historical statistics over the past five years. Any abnormal decrease (which should be predefined in the knowledge base) in the turnover may suggest a slow-moving or obsolete inventory.

(6) **Client's long-term purchase contracts with major vendors**: In general, integrated production techniques (e.g. Just-in-Time inventory system) requires the negotiation of long-term contracts with major vendors. The most important contents in a long-term contract include the qualifications and quality of goods, terms of payment, delivery or transportation policy, and goods-returning provisions. These contract contents serve as guidelines for the knowledge-based system to determine inventory costs and identify liabilities for purchase commitments.

(7) **Materiality levels for inventory, accounts payable, and various expenses**: Similarly, the knowledge-based system will revise these materiality levels periodically or continuously based on the audit results from previous audits.

(8) **Weaknesses and other significant problems found**: Internal control weaknesses and other significant problems included in the reportable condition letters and auditor's communications to the client's audit committee from previous audits are recorded. During a system audit, the auditor may periodically or continuously use the knowledge-based system to select random samples from the transaction logs to test whether the client has taken action on the weaknesses of its internal controls found in previous audits.

In light of the importance of knowledge-based system in the overall CAPS, two processing control issues should be addressed. First, since there are different knowledge bases and audit databases for different clients, the knowledge-based system should ensure that only the correct knowledge base and audit database are used for analyzing a specific client. The system may use a client ID to cross-link the retrieved transaction log files and their corresponding knowledge base and audit database. Second, the system needs control procedures to ensure that all the unmarked transactions in the log files are analyzed. In general, batch control totals can help determine the completeness of processing unmarked transactions. In addition to these control issues, the knowledge-based system should also have general control procedures to protect the knowledge bases and audit databases from being illegally modified or accessed by unauthorized staff within the CPA firm. Effective methods include the use of some authentication systems, IC smart cards, or other security-control mechanisms.

The Data-presentation Layer

This layer provides operational and presentational user interfaces for the auditor to browse, navigate, and review final outcome summaries and related accounting information and documents. Alarms will be triggered and exception reports be generated if abnormal situations occur from comparing transactions against existing standards in the previous data analysis layer. For example, if the randomly selected vendor is one of the client's related parties and its account balance exceeds the predefined upper limit, an alarm will be presented to the auditor's browser in this presentation layer. The auditor will then provide feedback (e.g. an electronic reportable condition letter) to the client's audit committee for improvements or explanation.

The Continuous Audit Seal (CAS) and Other Issues

Once the auditor has examined the exception reports and concluded that there is no material misstatement in the client's financial reports and transaction logs, the auditor may attach credibility to the client's financial information that will be disseminated to the public through the Internet. A *Continuous Audit* seal of attestation (which may be similar to the AICPA's *WebTrust* seal of assurance) is necessary to inform the public of the following:

(1) The auditor has examined and evaluated whether the financial information posted on the client's Web site is in conformity with the *Continuous Audit Principles.*
(2) The auditor has issued an audit report indicating that such principles are being followed in conformity with the *generally accepted electronic auditing standards (GAEAS).*
(3) To whom the seal was issued.
(4) Where the client awarded the seal is located.

This seal can be displayed on the client's financial information homepage together with links to the auditor's report and other relevant information.[15] The Web users who wish to make sure that a company has earned its seal can click on the seal itself and go directly to an independent authority's Web page (which may be similar to *VeriSign*) to confirm the company's status as a recipient of the seal. Furthermore, a few points should be noted for the disseminated financial information and the CAS auditor report. First, since it is almost impossible for a company to disclose a full set of financial statements every week or month, a business entity will only disclose key financial information on its Web site. Second, the audit procedures the auditor carries out for a continuous audit may not be sufficient to express an opinion on the fairness of all financial statement items. Third, the audit report should identify the subject of the report, indicate the audit procedures performed, state the auditor's findings, disclaim an opinion, and indicate that the audit report does not extend to the client's financial statements taken as a whole.

In light of the fast growing of real-time financial reporting, the CPA profession does need new auditing standards to guide the performance of continuous audits and the issuance of attestation seal and audit report on client's real-time financial information. Unfortunately, there is still a lack of new auditing rules such as the *Continuous Audit* seal of attestation, the *Continuous Audit Principles*, and the *GAEAS*. We believe that these areas deserve more comprehensive exploration to facilitate the continuous auditing in the future. The AICPA and CICA (1999d) report on continuous auditing has clearly indicated the requirements of a continuous audit and marked a first step effort in this direction.

Ultimately, the CAPM proposed in this section intends not only to ensure integrity and effectiveness of the entire accounting system but also to guarantee the correctness and use-

[15] While the *CPA WebTrust* seal provides periodical assurance on whether a Web site institutes EC practices to protect consumer interests, the *Continuous Audit* seal attaches continuous credibility to firms' financial information disseminated on the Internet.

fulness of the constantly generated financial statements for public dissemination. Once the continuous auditing process is carried out, the transaction trails and the client's AIS operations can be verified and validated on a continuous basis, leading to a constant dissemination of financial statements with high credibility.

SUMMARY AND CONCLUSIONS

Due to recent advances in network technologies and the enhancement of cost effectiveness by using Internet and World Wide Web applications, the development and practice of electronic commerce have grown rapidly. Almost all major business activities across various business domains can be set up in the internationalized, virtual, and electronic business environment with the aid of Web-based transaction and payment mechanisms. The main purposes of this paper have been twofold. First, this study identified possible impacts of EC on the auditing practices with a view to future development, challenges and opportunities. New audit risks and internal control considerations were discussed. Second, this paper proposed two new auditing process models that incorporate modern network security techniques and showed how an audit of a typical acquisition cycle can be conducted in an EC environment. A vendor invoice example was provided to demonstrate the approaches for auditing electronic evidence and supporting real-time information dissemination. The main contribution of this paper is that we propose a conceptual framework and corresponding solution processes for validating electronic transactions and for conducting external continuous auditing in an EC environment. In particular, our CAPM provides a first step to answer several issues proposed by Kogan *et al.* (1999) related to *continuous online auditing* (COA) (e.g. the architecture of COA, system audit, security of COA, and electronic records).

Three regulation issues that have been omitted in our discussion deserve further research. First, it is important to have legal rules guiding the separation and designation of duties on the development, modification, and control of invoice applications between the CA and the vendor. Second, the role and legal responsibility of the CA at the stage of invoice validation should be specified. Finally, since companies will disclose their financial information to the public on a real-time and continuous basis, there should be a set of *generally accepted electronic principles* (GAEP) that specify the content and format, the time interval and frequency, and the amount and extent of such disclosures.[16]

Acknowledgements

We would like to thank Dan O'Leary, anonymous reviewers of this article, and workshop participants at the National Chengchi University and the 7th Annual Research Workshop on Artificial Intelligence and Emerging Technologies in Accounting, Auditing and Tax (in conjunction with the 1998 AAA annual meeting) for their valuable comments on an early version of this paper.

References

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). Electronic Commerce Assurance Services Task Force. 1999a. *WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce* (February). Version 1.1.

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). Systems Reliability Task Force. 1999b. *SysTrust Principles and Criteria for Systems Reliability* (July). Version 1.0.

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). Electronic Commerce Assurance Services Task Force. 1999c. *WebTrust-ISP Principles and Criteria for Internet Service Providers in Electronic Commerce* (August). Version 1.0.

American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). Study Group on Continuous

[16] Recently, the SEC Practice Section Professional Issues Task Force released Practice Alert 97–1, *Financial Statements on the Internet*, to provide general guidelines for the dissemination of accounting information on the Internet.

Auditing. 1999d. *Continuous Auditing*. The Canadian Institute of Chartered Accountants: Toronto, CA.

American Institute of Certified Public Accountants (AICPA). 1983. *Statement of Auditing Standards, No. 47. Audit Risk and Materiality in Conducting an Audit*. AICPA: New York.

American Institute of Certified Public Accountants (AICPA). 1988. *Statement of Auditing Standards, No. 56. Analytical Procedures*. AICPA: New York.

American Institute of Certified Public Accountants (AICPA). 1995. *Statement of Auditing Standards, No. 78. Consideration of Internal Control in a Financial Statement Audit*. AICPA: New York.

Ansary HJ. 1993. The significance of EDI to corporate survival in the 1990s. *The Journal of Electronic Data Interchange* **6**(1): 10–13.

Bailey AD Jr, Duke GL, Gerlach J, Ko C, Meservy RD, Whinston AB. 1985. TICOM and the analysis of internal controls. *The Accounting Review* **LX**: No. 2, April, 186–201.

Bhimani A. 1996. Securing the commercial Internet. *Communications of the ACM* **39**(6): June, 29–35.

Borenstein NS *et al*. 1996. Perils and pitfalls of practical cybercommerce. *Communications of the ACM* **39**(6): June, 36–44.

Bruce DG. 1990. The future of EDI. *The EDP Auditor Journal* **1**: 11–13.

Bushaus D. 1991. EDI Billing Standard. *Communications Week* 13 May.

Camp LJ, Sirbu M. 1997. Critical issues in Internet commerce. *IEEE Communications Magazine* **35**: May, 58–62.

Canadian Institute of Chartered Accountants (CICA). 1993. *EDI for Managers and Auditors*. 2nd edn. CICA: Toronto.

Canadian Institute of Chartered Accountants (CICA). 1996. *Audit Implications of EDI*. CICA: Toronto.

Carroll M. 1997. Internet-commerce security. *Byte* **22**(5): May, 40IS25–40IS28.

Chalmer LS. 1990. Data security and control — new technology introduces new risks. *Journal of Accounting & EDP* Winter, 28–30.

Chan S. 1991. Managing and auditing EDI systems development. *CMA Magazine* November, 12–15.

Chang AM, Bailey AD Jr, Whinston AB. 1993. Multi-auditor decision making on internal control system reliability: a default reasoning approach. *Auditing: A Journal of Practice & Theory* **12**(2): Fall, 1–21.

Cobb S. 1996. Auditor, firefighter, lumberjack. *IS Audit & Control Journal* **1**: 36–39.

Cohen JB. 1997. Web audits: a complex art. *Editor & Publisher* **30**(6): 8 February 24i-27i.

Eckerson W. 1991. Car industry mulls move to EDIFACT. *Network World* 27 May.

Elliott RK. 1995. The future of assurance services: implications for academia. *Accounting Horizon* **9**(4): December, 118–127.

Emmelhainz MA. 1993. *Electronic Data Interchange: A Total Management Guide*, 2nd edn. Van Nostrand Reinhold: New York.

Fellen EW. 1997. Webware security. *Communications of the ACM* **40**(4): April, 130.

Frook JE. 1995. Web-hit audit system called into question. *Communications Week*. 18 December, 1, 60.

Graham JR. 1996. How to market and sell in a cyberworld. *Direct Marketing* **59**(6): October, 26–27.

Gunther LJ. 1994. Implementing EDI in a controlled environment. *IS Audit & Control Journal* **2**: 42–46.

Halper FB, Snively J, Vasarhelyi MA. 1992. The continuous process audit system: knowledge acquisition and representation. *EDPACS* **20**(4): October, 1–13.

Hansen J, Hill N. 1989. Control and audit of electronic data interchange. *MIS Quarterly* December, 403–413.

Herringshaw C. 1997. Detecting attacks on networks. *IEEE Computer* **30**(12): December 16–17.

Jones P. 1992. *Essentials of EDI Laws*. EDI Council of Canada Library Publication: Toronto, Canada.

Kalakota R, Whinston AB. 1996. *Electronic Commerce: A Manager's Guide*. Addison-Wesley: Reading MA.

Klur D. 1997. What an organization should know about using electronic cash. *Information Strategy: The Executive's Journal* **13**(3): Spring, 15–22.

Kogan A, Sudit EF, Vasarhelyi MA. 1996. Implications of Internet technology: on-line auditing and cryptography. *IS Audit & Control Journal* **3**: 42–47.

Kogan A, Sudit EF, Vasarhelyi MA. 1999. Continuous online auditing: a program or research. *Journal of Information Systems* **13**(2): Fall, 87–104.

Landsittel DL, Bedard JC. 1997. Fraud and the auditor: current developments and ongoing challenges. *The Auditor's Report* **21**(1): Fall, 3–4.

Liu C, Arnett KP, Capella LM, Beatty RC. 1997. Websites of the *Fortune 500* companies: facing customers through homepages. *Information Management* **31**(6): January, 335–345.

Marcella A, Sampias W, Kincaid J. 1992. Audit and control issues surrounding electronic data interchange. *EDI Forum* **1**: 48–52.

Marcella A, Chan S. 1993. *EDI Security, Control, and Audit*. Artech House: Boston, MA.

Meier JJ. 1992. EDI—A practical approach. *CMA Magazine* September, 29–31.

Meservy RD, Bailey AD, Johnson PE. 1986. Internal control evaluation: a computational model of the review process. *Auditing: A Journal of Practice and Theory* **6**(1): Fall, 44–74.

Panurach P. 1996. Money in electronic commerce: digital cash, electronic fund transfer, and E-cash. *Communications of the ACM* **39**(6): June, 45–50.

Pany K. 1998. ASB update as of May 15, 1998. *The Auditor's Report* **21**(3): Summer, 3–4.

Piven J. 1997. Resellers get set for SET. *Computer Technology Review* Spring, 28–31.

Pyle R. 1996. Electronic commerce and the Internet. *Communications of the ACM* **39**(6): June, 22–23.

Rittenberg LE, Schwieger BJ. 1997. *Auditing: Concepts for a Changing Environment*, 2nd edn. Dryden Press: New York.

Rubin AD, Geer DE Jr. 1998. A survey of Web security. *IEEE Computer* 31(9): September, 36–41.

Sivori JR. 1996. Evaluated receipts and settlement at Bell Atlantic. *Communications of the ACM* **39**(6): June, 24–28.

Tenenbaum JM, Chowdhry TS, Hughes C. 1997. Eco System: an internet commerce architecture. *IEEE Computer* **30**(5): May 48–55.

Vasarhelyi MA, Halper FB, Ezawa KJ. 1991. The continuous process audit system: a UNIX-based auditing tool. *The EDP Auditor Journal* **3**: 85–91.

Walden I, Braganza A. 1993. *EDI: Audit and Control*. NCC Blackwell: Oxford.

Wise TM. 1989. EDI: progressing toward the paperless office. *Internal Auditing* **5**(1): Summer, 75–81.

Wheatman V. 1991. Is X.435 the EDI interconnection solution? *Network World* 1 July, 24.

Wright B. 1992. The taxman has spoken: IRS Rule 91–59. *EDI Forum* (Recordkeeping Issue, Special Edition) June, 71–75.