CRITICAL ISSUES IN INTERNATIONAL AND ELECTRONIC AUDIT EVIDENCE

Author's details:

[1]Josiah, Mary and 2Izedonmi, P. F

[1]Igbinedion University Okada, Accounting Department,

College of Business 7and Management Studies

[2] University of Benin, Accounting Department,

Faculty of Business and Management Science.

ABSTRACT: *This paper is to examine the critical issues in international and electronic audit evidence. As entities process more data electronically, auditors should consider the validity completeness and integrity of such evidence. Today the development and convergences of information system allow for the saemless flow of information. Paperless environment are common place and in this context auditors gather electronic information as audit evidence. There are differences between paper work and electronic audit evidence. Auditors should focus on security issues by checking if the outsourcer shares valuable data and identify specific, local controls to prevent fraud and abuse especially when confidential information exist.*

Introduction

Electronic audit's evidences are increasingly used into practice of auditing as a new kind of evidence. Auditors are working in an increasingly digital environment since audit work essentially consists of gathering audit evidence to support the content of the audit report. The fact that documentary and other evidence used as competent evidential matter for the audit is in electronic format impact on the nature, format, reliability accessibility and sources and sources of such evidence that is on the entire audit process electronic audit evidence addresses the numerous issues auditors face in this environment. In the past, automation affected only some aspects of information processing.

Today,the development and convergence of IT and the integration of information system allow for the seamless flow of information paperless environment are commonplace and in this context auditors have to gather electronic information as audit evidence. Accumulating sufficient evidence needed to construct an informed decision means understanding where to look for that evidence. As entities process more data electronically, auditors should consider the validity completeness and integrity of such evidence.

Auditors, whose clients transmit, process, maintain or access significant amount of electronic information to test the adequacy of such controls normally – or either quality or disclaim an audit opinion. Accounting data now includes electronic equivalents of general and subsidiary ledgers, electronic fund transfer, invoices, contracts, and other relevant information with some of it only available in electronic form.

Objective of the study

The following are the objectives of electronic audit evidence.

1. To identified and defines electronic audit evidence, its attributes and determine how it differs from tradition audit evidence.
2. Identifies the impact of using electronic audit evidence to support the content of the audit report, particularly as regard, the audit the controls that may help mitigate the risks.
3. Identifies the tools and audit procedures available to audit control.
4. To indicate the other implication on the performance of audit procedure and examine the legal issues related to electronic audit evidence.
5. Recommendation based on our

finding.

LITERATURE REVIEW

According to Andree and Caroline (2011) states that using information technologies and computer systems to gather, process, transmit, maintain and present information is nothing new. What is new is an added dimension. In the past, automation affected only some aspects of information processing. To day ,the development and convergence of IT and the integration of information systems allow for the seamless flow of information. An integrated IS environment is a paperless environment where information is exchanged without space constraints and transmitted from one application to another, one entity to another, or one country to another via electronic networks.

Paperless environments are commonplace and in this context auditors have to gather electronic information as audit evidence.What is electronic audit evidence (EAE)? What are its attributes? How does it differ from traditional audit evidence? How does it impact the audit approach? What are the risks and the controls that can be applied to reduce them? These questions will be addressed.

EAE has an impact on the reliability of evidence and professional competence, knowledge of the entity's business, the audit approach, detection of misstatements and illegal acts and documentation of audit evidence. The report will set out recommendations for assurance standards to provide guidance on these issues and will deal with the risks of using EAE, the controls and technologies that may mitigate these risks, and the legal issues deriving from the use of electronic documents (e-documents) and signatures.

EAE is information created, transmitted, processed, recorded, and/or maintained electronically that supports the content of an audit report. The information can only be accessed using proper equipment and technologies such as a computer, software, printer, scanner, sensor or magnetic media. E-documents may take such forms as text, images, audio or video. EAE includes accounting records, sources documents and such vouchers as electronic contracts, e-documents pertaining to billing, procurement and payment, electronic confirmations and all other electronic data pertinent to the audit.

EAE differs from traditional audit evidence in several respects. First, it consists of information in a digital format whose logical structure is independent of the information. Second, the information's origin, destination and sent and received dates are not an

integral part of the e-document, message or other information format.

The more integrated the IS, the more business transactions will be processed and documented solely by electronic means. Auditors are most likely to use EAE internal and external integrated IS environments – for example e-environments include the entity's dependence on its own IS and on those of its partners and third-party service providers, together with the risk of failure at each of these levels. Other risks are loss of integrity, non-authentication, repudiation and violation of confidentiality of data, as well as loss of an adequate audit trail, and legal uncertainties.

PAPER VERSUS ELECTRONIC

Paper versus electronic

Paper audit evidence	Electronic audit evidence
Origin	
Proof or origin easily established	Proof of origin difficult to establish solely by examining electronic information. It is determined using controls and security techniques that allow for authentication and non-repudiation.
Alteration	
Paper evidence difficult to alter without detection	Alterations difficult, if not impossible, to detect solely by examining the electronic information. Information integrity depends on reliable controls and security techniques.
Approval	
Paper documents show proof of approval on their face	approval difficult to establish solely by examining the electronic information. It is determined using controls and security techniques.
Completeness	
All relevant terms of a transaction usually included In one same document	relevant terms often contained in several data files.
Reading	
No equipment needed	various technologies and equipment need.
Format	
Integral part of document	Separate from data and can be changed.
Availability and accessibility	
Not usually a constraint during the audit	Audit trail for electronic data may not be available at the time of the audit and accessing the data may prove more difficult.
Signature	
Simple matter to sign a paper document	appropriate technologies are required to

	And review the signature.	issue a reliable electronic signature and review it.
Clarity	Paper evidence is usually clear and Leads to the same conclusions by Different auditors controls	Electronic evidence is not as clear leads to and may lead to different conclusion depending on the procedures used and implemented.
Ease of use	Paper evidence does not require knowledge of Special tools to use in evaluating And understanding the evidence	Electronic evidence may require of data extraction techniques to evaluate and understand the evidence.
Prima facie credibility	Paper documents have a high Degree of credibility	Electronic evidence's credibility depends highly on the effectiveness of internal control structure.

Assessing reliability of electronic information as audit evidence

Authentication	The identity of the person or entity that created the information can be confirmed.
Integrity	the completeness, accuracy, current nature and validity of the information integrity is the assurance that the information was validated and was not intentionally or accidentally altered or destroyed when it was created, processed, transmitted, maintained and/or achieved.
Authorization	the information was prepared, processed, amended, corrected, sent, received and accessed by persons entitled to do so or responsible for doing so.
Non-repudiation	A party, person or entity having sent or received an information cannot deny having taken part in the exchange and repudiate the information content. Depending on whether there is irrefutable proof of origin, receipt or content of the electronic information, there is non-repudiation of origin, non-repudiation of receipt or non-repudiation of content.

To assess the sufficiency and appropriateness of the EAE gathered to support the audit report, the auditor should consider the specific risks associated with the use of such evidence. These can't be assessed solely by reviewing the documentary evidence, as is usually the case with paper documents. A printout of the

electronic information, or onscreen reading, is only one format. And it provides no indication of origin and authorization, nor does it ensure the integrity or completeness of the information. Auditors should ensure that controls and technologies to create, process, transmit and maintain electronic information are sufficient to guarantee its reliability. The importance of each criterion depends on the nature and origin of the electronic information and its intended use for audit purposes. In addition to assessing reliability of audit evidence ,the auditor looks into the availability of electronic evidence for audit purposes. Data confidentiality is also of interest to the auditor as a breach of confidentiality could represent a business risk that could impact the entity's financial position.

The reliability of electronic information depends on the reliability of the IS and supporting technologies. Where significant information underlying one or more assertions in financial statements is gathered, processed, recorded or maintained electronically, it may be impossible to reduce detection risk to an acceptable level by relying solely on the application of substantive procedures. In such cases, there is a high risk that misstatements in the electronic information obtained as audit evidence may not be detected. The auditor may need to adopt a combined approach and perform tests of controls to get appropriate audit evidence.

Because signing documents takes on a new dimension in an electronic environment, this issue needs to be examined closely. A signature primarily functions as a symbol signifying the signer's intention and authenticating the document**.** A handwritten signature on a paper document is affixed by an identifiable person and is intended to authenticate the intention inherent in the signed document. In a virtual environment, the signer cannot be identified visually. That is why the signature has to be used to confirm consent and to identify the signer. When a handwritten signature is affixed on a paper document, it is "merged" so to speak with that document. Since electronic information can migrate easily from one medium to another ,the signature and the document are independent of one another. The signature has to be bound with a specific document and the document's integrity needs to be established. The objective is to reduce the legal uncertainty as to the electronic signature's admissibility.

Electronic signature is a generic term to describe a technology-neutral signature in electronic and binary form. It may take various forms and be created in different ways. It may be created without any controls (a name typed at the end of a document); created using non-cryptographic security techniques (password, PIN number, biometric ID, digitized signature), or created using cryptographic security techniques (symmetric or secret key cryptography, asymmetric or public key cryptography or a digital signature).

Relevant controls and technologies must be used to obtain a reliable electronic signature. Non-cryptographic security techniques, based on a shared secret, help control authentication and authorization of the electronic document and signature. However, these security methods have limitations. Shared secret authentication supposes that the parties have already exchanged information to agree on the secret. Moreover, a secret is only effective if it hasn't been forgotten or discovered. Non-cryptographic security techniques offer no security as to the non-repudiation, integrity or confidentiality of e-documents and signatures.

Cryptographic security techniques, on the other hand, offer a secure way to ensure the authentication, non-repudiation, integrity and/or confidentiality. Non-cryptographic and cryptographic security techniques are often used to deliver a high level of reliability.

Digital signatures are based on asymmetric or public key cryptography. This technique involves mathematically generating a related key pair and using it to encrypt or decrypt data. One of the keys is kept secret by its holder, the other is freely available. The digital signature is generated by calculating a message digest and encrypting it with the signer's private key. The message digest is a unique number calculated using a hashing algorithm. This is a unique way to represent messages of varying lengths in much smaller format. If only one character of the original message is changed the message digest will be changed. If the value of the message digest calculated on the message received is identical to the original message, the authentication, non-repudiation and integrity of the message are ensured. However, assurance as to the signer's identity largely depends on the controls implemented to guarantee the security of the signer's private key and on the receiver's confidence that the identity associated with the public key is authentic. A public key infrastructure is a solution that may ensure sound key management and provide assurance as to the signer's identity.

Clearly electronic information raises important issues of interest to management, which needs reliable decision-making information, and auditors, who rely on this information to gather sufficient and appropriate audit evidence to support the content of the audit report.

Ever increasing information technology and organizational computer use require auditors to obtain evidence electronically and thus encourage the profession to incorporate the concept of electronic evidence into its professional standards. Financial statements of more and more firms using computers to process transactions. As evidence becomes more electronic (leaving fewer trails), auditors must change their audit techniques (Mancuso, 1997). This new auditing guidance on information technology suggests that auditors consider using continuous auditing when most information exists only in electronic form. We examine key auditing issues of new information technology including electronic evidence and internal control considerations.

Evidential matter

In guiding auditors along the information superhighway into the age of information technology, provisions incorporate the concept of evidential matter to help audit transactions in electronic form. As they obtain "sufficient competent evidential matter as part of the third standard of file work, auditors must assess management's assertions of underlying financial data presented in their published financial statement. Retains the basic relationship of Evidential Matter – underlying accounting data + corroborating information; but changes the nature of such evidential matter.

As entities process more data electronically auditors should consider the validity completeness and integrity of such evidence. Auditors whose clients transmit, process, maintain or access significant amounts of electronic information to test the adequacy of such controls normally – or either quality or disclaim an audit opinion. Accounting data now includes electronic equivalents of general and subsidiary ledgers, electronic fund transfers, invoices, contracts and other relevant information with some of it only available in electronic form.

Electronic messages may replace certain source documents such as purchase orders bills of lading, invoices and checks – in an electronic data interchange (EDI) or image processing systems. With EDI, an entity and its customers of suppliers use communication links to transact business electronically, but some electronic evidence may exist for only a "short time" and be irretrievable after a specified period if files are changed and backup files do not exist. Thus, auditors should consider the time during which information exists or is available in determining the nature timing and extent of their substantive tests and applicable tests of controls (Carmichael 1995).

Credible evidence stems from the independence of the source and the auditor's ability to corroborate that evidence including such factors as:

- Completeness of transaction's documents whose essential terms verify its validity.
- Ease of use which help evaluate and under stand evidence.
- Clarity noting that competent evidence should allow the same conclusions to be drawn by different auditors performing the same task.

In planning their work auditors should also recognize the competence presentation and specific EDP audit factors, including that:

- Potential errors include data transmission errors and deliberate data manipulation.
- Embedded control performance deals with unexpected changes to the data, and implied control performance deals with expected changes to the data.
- Limited access to or retention of electronic evidence may require the auditor to select samples several times during the audit period rather than just at year end.

Electronic evidence

Electronic evidence contains four basic forms of information text data, video and voice. While its intended purpose parallels that of traditional evidence, electronic evidence like traditional evidence raises issues regarding the evidence's validity completeness and integrity – and requires more pronounced control needs than does traditional evidence. Electronic evidence in EDP systems has not necessarily replaced traditional evidence in every system. "Information technology can be a source of electronic evidence or simply a repository of traditional evidence". Electronic evidence is defined as information transmitted processed maintained or accessed by electronic means and used by an auditor to evaluate financial statement assertions". Electronic evidence adds now dimensions for auditors to consider such as the reliability of the system producing and controlling the evidence. Electronic evidence generally depends on information technology for its creation which can help produce traditional evidence such as printed reports, and vice versa. A purchase order processed electronically is electronic evidence. Entering this approval in computer system again creates new electronic evidence.

The APS provides auditors with non authoritative guidance to compares and contrasts traditional and electronic evidence in context of several desired attributes of audit evidence.

As Table has 1 shown, attributes of traditional paper and electronic evidence differ greatly from one another auditors

should consider such key evaluative issues as:

- Electronic information as competent evidence. To verify the competence of evidence auditors should consider its validity completeness and other attributes. The traditional approach should also be considered when a lack of controls exists.
- Presentation of electronic evidence: Presentation of the same electronic information can take different forms and hence, auditors should perform appropriate procedures to ensure the consistency of presentations and consider the broader picture since all the information may be unavailable on one screen. The auditor should grasp how electronic evidence is extracted and test the consistency of presentation.
- Competence of tools used to access electronic evidence: Tools used to access electronic evidence should be well tested and checked for logical errors. Computer assisted audit techniques can expand the ability to analyze data recognize patterns, and test the assertions contained in financial statements.
- Definition of errors: electronic evidence allows for undetected changes that increase audit risks – including transmission errors or deliberate manipulation of data. Error detection routines enhance the effectiveness of internal controls. To access the effectiveness of control activities, auditors may perform tests of controls. Testing "through" the entity's information technology is more likely to be effective.
- Embedded or implied control performance: Detection of errors address unexpected changes that occur to the data, while internal controls address expected changes to the data. Alternative or traditional tests of controls may be needed for evidence that does not appear with the transactions.

The information superhighway

According to Glover and Romney (1997) some major impacts on auditing technology that occurred in the last decade include:

- Most frequent use of word processing and spreadsheet programs.
- Technology streamlining human resources needs.
- Rising electronic communication capabilities.
- An evolving internal auditor role to provide such value added services as developing improved, standardized processes, showing management how to perform control self-assessments, performing financial function reviews and risk assessments; accessing more information with less disruption to users and rendering improved ways to gather and analyze data to make "better" decisions.
- Continuous monitoring becoming feasible
- More prevalent electronic work papers.
- Improved sampling procedures because of more powerful EDP techniques.

Increasing importance of controls

Evidential matter in electronic form may impair auditors from reducing detection risk to an acceptable level by only performing

substantive tests – requiring additional tests of client controls. Changing technologies' have increased the importance auditors, managers and accountants give to internal controls. Thus, some documents to strengthen internal controls (Colbert and Bowen, 1996; Lainhart, 1996; Louwers and Pasewark, 1966; Gallegos and Powell) include:

- Information systems audit and control foundation's control objectives for information and related technology.
- Institute of internal auditors research foundation's system auditability and control.
- Committee of sponsoring organizations of the tread way commission's internal control integrated framework.
- The AICPA's consideration of internal control structure in a financial statement audit as amended by consideration of internal control in a financial statement audit.

Auditing implications and controls in major technological areas

In planning their work, auditors should consider the 11 key audit issues of new technologies this including security, electronic commerce, continuous auditing, Internet, EDI, image processing, communications technology Y2K issues, outsourcing, cooperative client/server environment and paperless auditing.

Electronic data interchange

EDI component of electronic commerce enables computers to communicate with one another. It requires trading partners to agree to use a specific standard data format to conduct their business transactions in an electronic fashion. Since little or no paper documents exist, auditors should concentrate on the computer system itself. While auditing such a seemingly complex system as EDI without paper trials may seem difficult, its general audit objective remains unchanged EDI systems still rely on testing for effective controls versus substantive testing.

EDI presents auditors with several audit and control implications when auditing paperless accounting systems. After grasping how their clients conduct business using EDI auditors should modify their audit plans and procedures.EDI systems audits generally include the following steps (Robertson and Louwers, 1999).

1. A familiarity of the business and information system.

2. Analysis of risks and development of audit programs based on risks identified.

3. Perform audit test.

4. Report findings

Auditors should become familiar with EDI systems and possess fundamental information system skills and should understand how businesses integrate various EDI systems and their plans for future growth. While EDI offers significant audit opportunities, some related risks include:

- Unauthorized intruders can intercept and change information that is communicated over public networks.
- EDI increases the dependency of 'trading partners' on one another to fulfil their information obligations.
- Disruptions in communications can cause some transactions be lost.
- Finding lost transactions becomes difficult especially in paperless environments.

- Greater reliance placed on computer controls can impede the effectiveness of internal control systems.
- Increased speed of individual transactions can make correcting errors in a timely manner difficult.
- Failure of one software component to affect the entire entity significantly and adversely.

Controls in EDI

Some Major Internal Control Considerations of an EDI system for auditors are that:

- Only authorized transactions are transmitted and received.
- They are not duplicated lost, or modified during processing, and
- Only authorized individuals have access to data.

Paperless EDI systems require auditors to use proper audit procedures to ascertain the adequacy and effectiveness of their client's internal controls. Systems also require adequate control built into them which can detect errors quickly and take action right away – since transactions occur continuously. Proper safeguards must always be in place. EDI control objectives and the activities to meet those objectives can be categorized as follows (Aggarwal and Hughes, 1996; Joseph and Engle, 1996; Rezaee and Aggarwal; 1996):

1. Timeliness
2. Accuracy and integrity
3. Security and
4. Recoverability/retention techniques, period processing and VAN message ware housing.

Timeliness refers to an auditor's timing in extracting evidence during the audit. Some evidence may exist or can be retained for only short times. Limited access to or retention of electronic evidence may require auditors to select samples several times during the audit period, rather than only at year end.

Auditors should competently grasp the accuracy and integrity of critical EDP evidence accumulated, in order to extract adequate factual and non misleading information. Those unsure about their ability to accumulate and evaluate electronic evidence properly should rely on outside specialists (Moreland, 1997).

New innovations in available security and applications controls the concurrent rise of computer use today, and new ways to access and manipulate them suggest that EDP systems consider such cost benefit tradeoffs as (Marsch, 1991):

- Unauthorized access to systems;
- Data accuracy and integrity
- Business interruptions
- Ability to recover from failure
- Systems that do not perform to needs
- Inefficient use of resources; and
- Lacks of skilled personnel.

Oz (1998) urges auditors to recognize areas of concern of such technological advances that relate to accumulating evidence on the effectiveness of controls. Table II lists some controls specific to each different level in the computer environment that auditors should consider in an electronic auditing environment.

Recoverability/retention techniques involve ensuring controls are in place to resume operations after business stoppages or interruptions due to computer error and being able to retain vital documents and evidence that were in the system before the breakdown. Auditors should determine if a business has a recovery plan in place. According to Oz (1998). "the plan should:

(1) be well defined and cover all options. (2) include preventive measures as well as procedures to implement in the event of disaster, and should minimize the number of decisions that must be made following the disaster, and (3) be set up of address the worst case scenario, but should permit parts of the plan to be executed when less severe disruptions occurred.

Client/server computing

The client/server model of system architecture has gained recent popularity – and contains three identifiable modules, the client or front end system containing the application software; a server or back end system containing the data; and middleware or the network that routes request for data from the client to the server. Client/server architecture allows end users access to centralized data from remote locations. Clients can retrieve only the data needed for the particular application. The client/server takes advantage of the central processing unit and random access memory of the PC processing, or distributes processing between the server and the client (Roesh and Henry, 1997).

Client/server systems contain some specific risks. Its environment duties are not always appropriately segregated, making some data easier to destroy. As developing time decreases and coding becomes easier and automated, testing and documentation of user created applications can become slack. New viruses can infect computers at various sites using network communication, and the security in network communications may be compromised.

Controls should be placed in the client/server environment to reduce these risks by focusing on both general and systems controls. As this is a three tier system, control activities are different for different tiers. Controls activities occur on the client side server side and the middleware. General controls are critical to the internal control structure of client/server architecture – as are control of access to programs and data and control of computer operations. When auditing client/server systems, auditors should examine the control environment, including management's involvement in setting policies the organization structure segregation of duties methods of storage and personnel policies as well as the control structure including the accuracy of transactions and records procedures followed for development of systems; and date conversion and access.

Systems wide control activities include authorizing procedures for system development documenting and testing plans, physical security over hardware and software, independent checks of C/S system, and periodic preventative maintenance. Client-side control activities include hardware and software locks, timed lockouts, limiting number of access attempts, programmed edit checks, error detection, correction and encryption capabilities, and automated backup of client applications.

Network activities critical for the C/S systems include monitoring network activities and network traffic, network operating systems software controls and using call back devices to authenticate users. Server activities include limited access, data security virus detection and diagnostic software sign on procedures and timed backups.

As entities focus more on their "core" competences, they increasingly rely on outside vendors (e.g. IBM, EDS and Andersen Consulting) or form organizational alliances to develop their information systems (IS). While outsourcing helps recue IT licensing fees,

shorten IT implementation cycles, reduce personnel costs and strengthen security, this process can also cause them to lose control of loyal) IS employees and can erode the entities competitive advantages in the IS arena.

In evaluating their clients' internal control systems in such outsourcing environments, auditors should focus on additional security measures, by reviewing the:

- general EDP controls of the outsourcer's data centers;
- Overall outsourcing agreements for contract compliance.
- Client billings and other measures of data center efficiency; and
- Extent of surety bonds or other devices to check on the outsourcers integrity (Simmons 1997).

Summary

Much progress has been made to legally recognize e-documents and signatures as evidential matter. Ottawa and most provinces have passed e-commerce legislation and have amended evidence acts to recognize e-documents and signatures and establish admissibility criteria for this evidence. However, there is still some legal uncertainty about e-documents. Major ambiguities persist regarding jurisdiction and laws applicable to cyber transactions. Some uncertainty remains about admissibility conditions for e-documents and signatures under Canadian law.

In cases where the admissibility of an e-documents is questioned, it is up to the person wanting the document admitted to establish its integrity and authenticity. It is up to the court whether the evidence is admissible. The best way for an entity to mitigate the legal risks associated with the admissibility of e-documents and establishes data integrity is to institute and maintain reliable IS and use appropriate technologies. The admissibility of an e-signature is also subject to certain conditions. The technology must allow for the identification of the signer, and the link between the signature and the e-document must be created in such a way that subsequent alterations of the document can be detected. In addition, some legislation sets out standards requiring the use of certain technologies or the application of specific procedures.

Recommendation

Auditors should also focus on security issues by checking if the outsourcer shares valuable data and identifying specific, local controls to prevent fraud and abuse-especially when confidential information exists.

Conclusion

As technological changes occur more quickly auditors must keep peace with emerging technological changes and their impacts on their client's data processing system as well as their own audit procedures. As intranet and extranet issues become more complicated auditors should also play a major role in all aspects of business. Most accounting transactions should soon be in electronic form without any paper documentation. The use of electronic commerce changes the way business transactions are processed and accordingly, the nature of audits. The future holds great challenges for auditors and riding full speed through the information superhighway will be the only way to face those challenges. We discuss some of these challenges and other technological issues auditors may face as their clients process more of their financial transactions on advanced electronic systems.

References

Aggarwal, R. and Hughes, C. (1996). "Internal control in system development with CASE". *Internal auditing* Vol;. 53. Winter, pp. 26-33.

American Institute of Certified Public Accountants (1980). *Evidential Matter Statement on Auditing Standards* (SAS) No. 31,August.

American Institute of Certified Public accountants (1988). *Consideration of the Internal control Structure in a financial audit*, SAS No. 55. April.

American Institute of Certified Public accountants (1995). *Consideration of Internal control in a financial Statement audit*: amendment to SAS No. 55, December.

American Institute of Certified Public accountants (1996). *Amendment to Statement on auditing Standards* No. 31, Evidential Matter, SAS No. 80 December.

American Institute of Certified Public Accountants (1997). The Information Technology Age Evidential Matter an Auditing Procedures Study.

Carmichael, D. (1995). "Business risk internal control and audit implication of EDI". *The CPA Journal* Vol. 65 November, pp. 56-61.

Colbert, J. and Bowen, P. (1996). "A comparison of internal controls: COBIT. SAC, COSo, SAS 55/78", IS *Audit and control Journal* Vol. 4 pp. 26-35.

Gallegos, F. and Powell, S. (1996). "Telecommunications networks in virtual corporations". IS *audit and control Journal* Vol. 3, pp. 26-8.

Glover, S. and Romney, M. (1997). "Software – 20 hot trends". *The Internal auditor,* Vol. 54 august, pp. 28-35.

Helms, C.. and Mancino, J. (1998). "The electronic auditor". *Journal of Accountancy,* April pp. 45-8.

Information systems audit and control foundation (1996). "COBIT control objectives for information and related technology", *IS Audit and control Journal*, Vol. 4 pp. 12-12.

Joseph, G. and Engle. T. (1996). "Controlling EDI environments consistent with COBIT and COSO". *IS audit and control Journal*, Vol. 4 pp. 36-41.

Lainhart, J. (1996). "Arrival of cOBIt helps refine the valuable role of IS audit and control in the enterprise". *IS audit and control Journal*, Vol. 4 pp. 20-3.

Louwers, T. and Pasewark, W. (1996). "The Internet: changing the way corporations tell their story". *The CPa Journal* Vol. 66 November pp. 24-8.

Mancuso,A. (1997). "Auditing Standard Board issues SAS No. 80". *The CPA Journal* Vol. 67 March. P.74.

Marsch,H.L. (1991). "SAC is back the new systems audit ability and control report". *Management Accounting* January pp. 57-60.

Moreland, K. (1997). "SAS 80 amends SAS 31 to address information technology". The Ohio CPA Journal, July-Sepetember pp. 47-9.

Oz, E. (1998). Management Information Systems, 1st ed. Course Technology Cambridge, MA. Prawitt, D. and Romney, M. (1997). "Emerging business technologies". *The Internal Auditor* vol. 54 February pp. 25-32.

Rezace, Z and Aggarwal, R. (1996). "EDI risk assessment". *The Internal auditor* Vol. 53 February pp. 40-4.

Robertson, J.C. and Louwers, T.J. (1999). Auditing 9th ed. Irwin McGraw Hill, Burr Ridge IL.

Roesh, L and Henry, I. (1997). "Client/server system". *Journal Auditing* vol. 5 august pp. 40-3.

Simmons, M. (1997). "The standards and the framework". *The Internal auditor* vol. 54 April, pp.50-5.