AUDITING

BUSINESS RISK, INTERNAL CONTROL, AND AUDIT IMPLICATIONS OF EDI

By Stanley Weiner

[Editor's Note: An extensive discussion of certain aspects of electronic data interchange (EDI) is included in this month's feature article "The IRS Regulatory Implications of Electronic Record Keeping" by Joseph Danos and Ram S. Sriram. It is accompanied by a sidebar by Mr. Weiner, which explains some of the basics of EDI. It is suggested readers familiarize themselves with the EDI concepts in the feature and the sidebar before proceeding with this article.]

Legal Aspects

In the past, EDI was limited to simply sending and receiving various messages. However, within the past few years, trading partners have allowed each other access to internal records such as sales and inventory information. This allows the selling partner to monitor stock usage and provide just-in-time inventory techniques. The customer, in effect, is permitting the selling partner to ship goods based upon a predefined agreement. It is important that, to protect both parties, any agreement be codified legally in what is known as a "trading partner agreement." A trading partner agreement normally includes the following major elements:

- EDI standards:
  - Transaction standards. This defines business transactions that will be conducted between trading partners. This also includes any restrictions, such as a limitation on the dollar amount of a particular type of transaction.
  - Message standards. This stipulates the form and content of messages. These will normally be ANSI ASC-X12 within the U.S.
  - Security Standars. Sensitive data is often transmitted. Consideration will have to be given as to how such information will be protected. Other issues, such as authentication and data integrity, will also have to be resolved.
  - Data storage standards. Trading partners will also have to agree upon the storage of sensitive data and the method and time frame of data retention.

Editor:
Douglas R. Carmichael, PhD, CPA
Baruch College

- Accountability—outlines the obligations of the trading partners.
- Standard of care—degree of diligence to be used by each trading partner.
- *Force majeure*—unexpected or unanticipated events.
- Message validation and error-check procedures.
- Security control—use of encryption, if required.
- Trade terms and conditions.
- Confidentiality—protection of proprietary information.
- Arbitration and dispute resolution.
- Governing law of the agreement.

EDI presents varied challenging legal issues. Attorneys will have to have experience in data processing and will have to interact with both accountants and technical data processing personnel.

Accounting Issues Related to the Use of the Internet

Many companies may evaluate the use of the Internet for the communication of transactions. At the present time, this should be avoided. The Internet is an unregulated environment and presents many dangers. The majority of computer crimes occur on the Internet. Furthermore, use of the Internet in many instances will eliminate the buffer that a value-added network provides. This means that unauthorized parties would have the opportunity to provide adequate audit trails and controls for the accountant to utilize. The Internet utilizes many networks. In certain instances, the efficiency and reliability of such networks are questionable.

Business Risk

Although EDI offers significant opportunities, it also has a number of business risks. Both financial managers and accountants should be aware of these risks to take appropriate action to minimize them during system planning and implementation. Some of the risks to be dealt with are the following:

Loss of Business Continuity. Corruption of EDI applications, whether done innocently or deliberately, could affect every EDI transaction undertaken by a company. This would have a negative impact on both customer and vendor relations. In an extreme situation, it could ultimately affect the ability of a company to stay in business.

Loss of Independence. The nature of EDI increases the dependency of trading partners upon one another to fulfill their obligations. For instance, failure of a vendor to meet its just-in-time inventory commitments could have a severe impact on its customer relationships, sales, and resulting cash flows.

Loss of Confidentiality of Sensitive Information. Proprietary information, such as customer lists, price lists, manufacturing schedules, etc., could fall into a competitor's possession.

Increased Exposure to Fraud. EDI reduces the segregation of duties and limits the number of personnel involved with individual transactions. Control of internal systems and procedures may be limited to a few people. This increases the risk of unauthorized transactions. For example, if internal control related to the new automated system is not adequate—

- fictitious customers could be paid,
- overpayments to existing vendors with subsequent kickbacks could occur, or
- payments for merchandise not received could take place.

Loss of Transactions. As a result of disruptions in communications or within internal systems, it is conceivable transactions could be lost. This could also create garbled messages and inaccurate data.

Loss of Audit Trail. An EDI system with a translation program reduces the need for hard copy. Once management gains confidence in the system, it will avail itself of this benefit. Audit procedures will have to be established to verify specific transactions contained in electronic media.

Potential Reduction in Internal Control. Greater reliance will be placed on computer controls. Systems management will utilize fewer more technically adept personnel. Also, the increased speed of individual transactions will make it difficult to correct errors in a timely manner. Management will have to understand and react to the increased exposure to unauthorized transactions and error.

Software Failure. Should any part of the system fail, management would have to confront problems related to transactions that have to be completed by set due dates. Types of transactions that could impact the organization include cash payments, payroll, just-in-time inventory, and production schedules.

Legal Liability. EDI is in its infancy. Case law related to this method of doing business is limited. Where responsibilities

of trading partners are not clearly defined by a trading partner agreement, there could be uncertainty related to specific legal liability.

Internal Control

Taking EDI to its end form of paperless transactions will pose challenges to both financial management as well as internal and external auditors. Assurance that internal control is adequate will require more sophisticated measures. The auditor who normally audits around the computer will have to develop techniques to audit through the computer system.

The following are some of the issues related to internal control that should be considered in the EDI installation:
■ Automation of controls will increase. Controls will be built into programs, and their use must be understood.
■ Errors must be identified and resolved more quickly. Without proper control, it is possible a transaction could be consummated before an error is discovered.
■ The accounting organization and processes will change. A paperless environment will require adjustment within the accounting department.
■ Transaction evidence will become mainly electronic. Such records could disappear if proper safeguards are not in place.
■ Security of the computer installation and system will have to be upgraded.

To address internal control issues, both the internal and external accountant should be included in the planning phase of the new system. The accountant should attempt to ensure all transactions are properly authorized and that they are complete, accurate and, valid. Controls should apply to both inbound and outbound transactions. Paperless authorization will require special access to authorization fields within the computer system. Provision should be made wherever possible for acknowledgment of transmissions.

As previously discussed, fewer personnel will be involved with transaction processing. Therefore, opportunities to review transactions will be reduced. For instance, payment of purchases will be based upon entries within the computer system that indicate the transaction was properly authorized and received.

Critical to the internal control function will be the capability to catch errors. The time span of a transaction will be significantly shortened. If system controls do not catch an error, it is possible that erroneous payment or shipment will be made.

Controls should also be in place to address the following risks:

Transmission Errors. These should

Phase Component	Explanation
TABLE EDI AUDIT APPROACH	
Knowledge	Gain knowledge of the EDI technology and the technical issues involved.
Personnel	Identify EDI personnel relevant to an audit investigation and gain an understanding of their responsibilities.
Location	Identify location of the EDI development efforts and EDI applications in production.
Impact	Determine the extent of EDI use and its impact on the organization and its strategic fit.
Development	Get involved in prime EDI network developments and undertake system development audit reviews.
Network provider	Assist in, and review choice of, EDI network provider and audit the EDI software selection process.
Management approach	Review the EDI planning, human resource project staffing, and management approach to the developments.
Document	Understand and document EDI components—how they interrelate and how the EDI system relates to other information systems technologies and applications.
Risks	Identify risks associated with the EDI environment and applications using EDI.
Security control & audit	Understand the types of security, control, and auditability mechanisms appropriate to the EDI environment.
Contingency planning	Review the EDI contingency planning approach documentation, personnel, and testing to ensure effective and adequate plans are in place should a disaster arise.
Evaluate	Evaluate EDI security, controls, and auditability mechanisms.
Third-party audit reports	Obtain a third-party audit report of the EDI Network service and value-added network if appropriate or available.
Legal	Review EDI documentation and legal considerations of EDI developments.
Audit evidence— tools & techniques	Gather audit evidence and consider the use of EDI audit tools and techniques in this process.
Development audit tools	Consider the use of in-built audit monitors or the development of integrated test facilities to help assist the auditors in this complex environment during EDI system development audits.
Test, evaluate, and conclude	Conclude evaluation after the results of compliance and substantive EDI tests are known.

Source: *An Audit Approach* , Rodger Jameson, The EDP Auditors' Foundation, Inc.

be addressed by the standards that indicate the message format and content are valid.

Translation Errors. Controls should be in place to ensure standard ANSI transmissions are properly converted for the application software by the translation application.

Reasonableness Checks. The receiving organization must have controls in place to test the reasonableness of messages received. This should be based upon a trading partner's transaction history or documentation received that substantiates special situations.

Manipulation of Data. Controls should be established to guard against manipulation of data in active transactions, files, and archives. Attempts to change records should be recorded by the system for management review and attention.

Only Authorized Messages Are Sent and Received. Procedures should be established to determine messages are only from authorized parties and that transmissions are properly authorized.

Audit Considerations

Internal or external auditors should be aware of the following considerations:

Technical Issues. The auditor should develop an understanding of the EDI system and its technical aspects.

Strategic Fit. An understanding of the role of the EDI function within the organization should be obtained. As part of obtaining an understanding of the internal control structure, this should be documented and flow charted.

Planning and Human Resources. The auditor should assess whether the EDI system meets management's plan and expectations. Should the system not be up to plan, it could create an internal control deficiency. The evaluation of the human resources allocated to the maintenance of the EDI system is also important. Control of the system will be limited and the auditor should assess the capability and reliability of system's personnel.

Audit of the Value-Added Network (VAN). The auditor should gain some knowledge and assurance that the controls and security provided by the VAN are effective. This is normally achieved through an audit of the VAN's procedures and controls by a qualified auditor who issues a report provided to all users.

Evaluate the Disaster Recovery Plan. The auditor should evaluate the organization's disaster recovery plan. This should not only include the entity being audited, but the value added network as well.

Retrieval and Testing of Audit Evidence. The issue of gathering audit evidence for testing will become increasingly more computer oriented. While hard copy generally exists currently, in the long term it is envisioned such medium will significantly decrease. The auditor will have to ensure that access to the entire population of transactions is available. Furthermore, the auditor will also have to gain assurance that data within the population under scrutiny has not been modified.

New Audit Tools and Techniques. To deal in a more sophisticated environment, the auditor will have to develop or utilize advanced audit techniques. Some of the methods to be considered include the following:

■ Audit software—Such software currently exists and can be utilized for a number of purposes. These include statistical sampling techniques, analysis and stratification of the population being examined, test of the mathematical accuracy of computer files, and extraction of data, based upon predetermined parameters, for further scrutiny.

■ Transaction verification by the VAN—Some value added networks will provide assistance in transaction verification. The cost and method should be investigated early in the audit period because VANs only keep data for a very short period of time.

■ Test of the EDI system—The EDI system can be tested by sending messages to the organization being audited through the VAN. Some VANs, for a fee, will also assist with this effort. Such tests could include communications links, system interfaces, translation software, and application software processing.

■ Audit monitors—Devices can be installed at EDI workstations to capture transactions as they are received. Such transactions can be stored in a protected file for use by the auditor. Consideration should be given to storage requirements for voluminous amounts of data.

■ Expert systems—Within the context of utilizing the computer system for internal control checks, consideration should be given to have "audit monitors" evaluate transactions received. Based upon judgmental rules, the system can determine the audit significance of such transactions and provide a report for the auditor's use.

As use of EDI becomes more widespread, additional methods for auditing transactions will be developed. It is important to stay current with these developments. ❏

Stanley Weiner, CPA, is a partner with Cornick Garber & Sandler, LLP.