EDI control: management and audit issues

Sally Chan

Follow this and additional works at: https://egrove.olemiss.edu/aicpa_guides

Part of the Accounting Commons, and the Taxation Commons

Recommended Citation
https://egrove.olemiss.edu/aicpa_guides/420
Notice to Readers

This book is sold with the understanding that neither the authors nor the publisher is hereby rendering legal, accounting, or other professional advice. If such advice or other assistance is required, the personal services of competent professional counsel should be sought. This book does not establish standards or preferred practice; it represents the opinion of the authors and does not necessarily reflect the policies of the AICPA or the Information Technology Division.

Richard D. Walker, Director
Information Technology Division

Nancy A. Cohen, Technical Manager
Information Technology Membership Section
EDI Control, Management, and Audit Issues

By S. Chan, M. Govindan, J.Y. Picard, G.S. Takach, and B. Wright

AICPA
American Institute of Certified Public Accountants
The introduction of electronic data interchange (EDI) into an organization's information system brings with it an entirely new set of problems and issues for executives, systems professionals, consultants, managers, and auditors. The transient nature of the audit trail, the resulting paperless environment, and the total dependence on systems to support operations — with little or no human intervention — significantly increase risk. Whether a manager or an auditor in an EDI environment, one cannot afford to be reactive and corrective after the fact.

This book provides proactive guidance for —

- The corporate manager facing changing business conditions and the resultant difficulties and risks.
- The internal auditor who must satisfy various mandates, including advice to management regarding the EDI environment.
- The external auditor who must have a thorough understanding of the ramifications of EDI in performing audits or reviews and in providing levels of assurance.
- Information systems professionals and consultants who are involved in the control dimensions of EDI.
- Line managers who must assume full managerial responsibility for all facets of EDI.

EDI for Managers and Auditors (second edition) has been reprinted and updated under the title EDI Control, Management, and Audit Issues with the permission of the Canadian Institute of Chartered Accountants. It was written by a team of specialist authors committed to covering the full spectrum of technology, management, control, auditability, law, review, reporting, disclosure, and levels of assurance. Two of the authors are lawyers with authority in both the United States and Canada, making this a true North American reference document. The original section on auditing EDI has been replaced to conform with U.S. auditing standards.

The Information Technology Division expresses its appreciation to Ken Fullerton, CPA, and the AICPA Auditing Standards Division for permission to reprint their material as Chapter 8, “EDI Effect on the Audit.”

Richard D. Walker, Director
Information Technology Division

Nancy A. Cohen, Technical Manager
Information Technology Membership Section
One of the most commonly asked questions by managers at our education courses is "How do we adequately control our EDI environment and satisfy senior management and our financial auditors in the use of EDI?" When EDI (electronic data interchange) is integrated into the business process, what tools can be made available to internal and external auditors to provide control assurance that simultaneously affords stakeholders a level of comfort and support for the corporate EDI business strategy?

More and more business transactions are exchanged through EDI. Hence, EDI's impact on the business environment is significant and does affect the control structure of the organization. Until now, little has been available on this subject, both in North America and around the world, but I am convinced that *EDI Control, Management, and Audit Issues* should be required reading for the business manager who has the responsibility of managing, controlling, and understanding all facets of the EDI process. This book should also be mandatory reading for auditors.

The EDI Council of Canada published the first edition, which was very well received by the membership. Given the nature of the material, it is no surprise that the financial audit profession would want to make this book a significant part of its curriculum of study and professional development for its members. Indeed, we are pleased to have worked with the authors and we endorse their efforts and congratulate them for their vision in making this work available to the profession and to EDI users around the world.

---

Marshall A. Spence, *President*

*Electronic Data Interchange Council of Canada*

Toronto, February 1995
# Table of Contents

## 1. Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whom This Book Is for</td>
<td>1</td>
</tr>
<tr>
<td>EDI Defined</td>
<td>2</td>
</tr>
<tr>
<td>EDI Infrastructure</td>
<td>3</td>
</tr>
<tr>
<td>Generating a Document</td>
<td>4</td>
</tr>
<tr>
<td>EDI Standard Formats</td>
<td>5</td>
</tr>
<tr>
<td>Accredited Standards Committee (ASC) of ANSI</td>
<td>5</td>
</tr>
<tr>
<td>International Standards Development UN/EDIFACT</td>
<td>5</td>
</tr>
<tr>
<td>Standards Limitations</td>
<td>7</td>
</tr>
<tr>
<td>The Most Current Update on Standards</td>
<td>7</td>
</tr>
<tr>
<td>Growth of EDI Technology</td>
<td>9</td>
</tr>
<tr>
<td>Trends in Software and Hardware Usage</td>
<td>9</td>
</tr>
<tr>
<td>New Dimensions for Managers</td>
<td>10</td>
</tr>
<tr>
<td>Internal Auditors as Consultants on Technology and Advisory on Control</td>
<td>10</td>
</tr>
<tr>
<td>Topdown Effect and Cluster Effect</td>
<td>10</td>
</tr>
<tr>
<td>New Dimensions for the External Auditor</td>
<td>11</td>
</tr>
<tr>
<td>Organization of the Book</td>
<td>11</td>
</tr>
<tr>
<td>Appendix: EDI Transmission and Control Structure</td>
<td>12</td>
</tr>
<tr>
<td>References</td>
<td>17</td>
</tr>
</tbody>
</table>

## Part One: The EDI Environment

## 2. The EDI Environment and Business Opportunities

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDI History</td>
<td>21</td>
</tr>
<tr>
<td>Key Industry Segments and Pioneers</td>
<td>22</td>
</tr>
<tr>
<td>Benefits of EDI</td>
<td>23</td>
</tr>
<tr>
<td>Window of Opportunities</td>
<td>25</td>
</tr>
<tr>
<td>EDI Gives Rise to Potential New Risks</td>
<td>25</td>
</tr>
<tr>
<td>References</td>
<td>29</td>
</tr>
</tbody>
</table>
### 3. Management Issues

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency, Effectiveness, and Economy</td>
<td>31</td>
</tr>
<tr>
<td>Objectives for Information Systems</td>
<td>32</td>
</tr>
<tr>
<td>Managing Change</td>
<td>32</td>
</tr>
<tr>
<td>Business Process Reengineering (BPR)</td>
<td>33</td>
</tr>
<tr>
<td>Pilot Mode Caution</td>
<td>34</td>
</tr>
<tr>
<td>Reorganization and Levels of Integration</td>
<td>34</td>
</tr>
<tr>
<td>Managing Trading Partners and Third Party Network Providers</td>
<td>35</td>
</tr>
<tr>
<td>Total Systems Dependence (TSD)</td>
<td>36</td>
</tr>
<tr>
<td>Monitoring, Control Data and Joint Ownership</td>
<td>39</td>
</tr>
<tr>
<td>Shift From Balance Sheet Focus to Operations</td>
<td>40</td>
</tr>
<tr>
<td>EDI Post-Installation Reviews</td>
<td>40</td>
</tr>
<tr>
<td>References</td>
<td>41</td>
</tr>
</tbody>
</table>

### 4. Security Technology

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDI Security and Control Objectives</td>
<td>44</td>
</tr>
<tr>
<td>Message Authentication Code (MAC)</td>
<td>45</td>
</tr>
<tr>
<td>Encryption</td>
<td>45</td>
</tr>
<tr>
<td>Hardware Encryption</td>
<td>45</td>
</tr>
<tr>
<td>Security Key Management</td>
<td>46</td>
</tr>
<tr>
<td>Automated Key Management</td>
<td>46</td>
</tr>
<tr>
<td>Manual Key Exchange</td>
<td>47</td>
</tr>
<tr>
<td>Security Incident Reporting</td>
<td>47</td>
</tr>
<tr>
<td>Control Significance to Managers and Auditors</td>
<td>48</td>
</tr>
<tr>
<td>References</td>
<td>49</td>
</tr>
</tbody>
</table>

### 5. Application Controls and Environmental Controls

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy and Completeness</td>
<td>51</td>
</tr>
<tr>
<td>Authorization Controls</td>
<td>54</td>
</tr>
<tr>
<td>Security</td>
<td>54</td>
</tr>
<tr>
<td>Auditability</td>
<td>56</td>
</tr>
<tr>
<td>Timeliness and Recoverability</td>
<td>57</td>
</tr>
<tr>
<td>Controls Surrounding Third Party Network Providers</td>
<td>58</td>
</tr>
<tr>
<td>Special Control Considerations for Financial EDI</td>
<td>59</td>
</tr>
<tr>
<td>ANSI ASC X12 Versus UN/EDIFACT Payment Format</td>
<td>61</td>
</tr>
<tr>
<td>The Canadian FEDI Audit Trail</td>
<td>62</td>
</tr>
<tr>
<td>Monitoring Systems and Control on Controls</td>
<td>63</td>
</tr>
<tr>
<td>Embedded Audit Modules (EAM)</td>
<td>64</td>
</tr>
<tr>
<td>Integrated Test Facility (ITF)</td>
<td>64</td>
</tr>
</tbody>
</table>
6. **Project Management and Package Evaluation**

The Emergence of Inter-Enterprise Systems
Implementation Issues
Project Management Issues — Lessons From Winners
The Auditor as Consultant
Package Evaluation
Sources for More Vendor Information
References

7. **Legal Issues in EDI Implementation**

Section I — The American Perspective
Trading Partner Agreements
Part A — Communication Terms
Part B — Trade Terms and Conditions
Evidence Law and Record Credibility
Record Retention and Control Requirements
Vendor Agreements
Special Regulations
The Role of Lawyers and Auditors

Section II — The Canadian Perspective
Contract Law Issues
Evidence Law Issues
Record Retention Issues
Trading Partner Agreements
Network Agreements
References
Appendix A: Trading Partner Agreement Model
Appendix B: IRS—Administrative, Procedural, and Miscellaneous
# Part Two: Auditing EDI

## 8. Electronic Data Interchange—Effect on the Audit

- Assessing Inherent Risk: 103
- Understanding the Internal Control Structure: 105
- Control Policies and Procedures: 105
- Tests of Controls: 109
- Assessing Control Risk: 109
- Designing Substantive Audit Procedures: 110
- Auditor's Recommendations to Clients: 112
- Summary: 112
- Appendix: Potential Substantive Procedures: 113
- References: 121

---

## Bibliography

## Glossary

## Abbreviations Used
Chapter 1. Introduction

Whom This Book Is for

The first edition of this book addressed controls, the management issues and levels of assurance from the perspective of compliance, and the function of the internal auditor. It also provided the internal auditor with adequate reference material to satisfy various mandates including advisory to management regarding the EDI (electronic data interchange) environment. This second edition proposes to include the concerns and the objectives of the external auditor as well. The interest and the concerns of management are discussed from a somewhat wider perspective. The important issues facing the corporate manager in the light of fast changing business conditions should be addressed. This is especially so, as applies to the use of technology as an avenue to a more effective presence in the marketplace. The globalization of markets, a general trend towards a regionalized economy, the impacts from maturing information technology, its pervasive nature, indeed represents simultaneously, significant pressure points to cope with, and brings into focus the requirement for sources of guidance, vision, and orientation.

Taken from the perspective of corporate managers, the level of difficulty and associated risks, are substantial. The primary reason, is that there is no past experience in history equivalent to the current situation to fall back on as a guide. An understanding of the mutating business environment along with a sense of vision, has never been more pressing. The mandate given to corporate management where uncertainties abound, and where past experiences count for less, gives rise to adverse situations totally unexpected just a few years ago. Consequently in these times of change, one would expect that an open mind be the basic requirement for imparting change in a positive way, not just to survive as a corporate entity but more so, reap the benefits of a better performing organization, which invariably finds its measurement in its economic bottom line.

While managers and auditors have different mandates, concerns, and objectives, one should not take the insular view of how within the overall social and economic context, they come to depend on virtually the same environmental factors and infrastructures. It becomes a matter of angles for points of view and emphasis, not a matter of differing substance.

This second edition can also be used as a practical guide by information systems professionals and consultants who are specifically interested in the control dimensions regarding Electronic Data Interchange (EDI). The premise underlying this work is that there is a need for a single reference document which ultimately would contain all the essential and pertinent informative material on the various management, legal, and audit aspects of EDI. The authors also believe that this document should be practical and immediately useful in making control decisions, and/or be adequately supportive when performing an audit in this rapidly growing sector.

Numerous books and articles on the subject of EDI have been produced over the past few years. By and large, these documents discuss the potential benefits that this technology has to offer, especially in managing the flow of information in a more cost-effective manner. These documents also touch upon the nature of business transactions between EDI trading partners, as well as some of the associated risks.

What has been mostly lacking, however, is a comprehensive reference tool which would provide both the necessary background examination of the new control, audit, and legal issues posed by EDI and the corresponding control and
EDI Control, Management, and Audit Issues

This book attempts to go some distance towards filling the gap, by addressing both the controls needed to realize the potential benefits of EDI and those needed to bring the levels of risk within a manageable tolerance. It is an earnest attempt to provide managers and auditors with the background and a practical tool to assess and appreciate the significance of the EDI environment, and its unique characteristics.

EDI Defined

EDI can be defined as an exchange of electronic business documents between economic trading partners, computer to computer, in a standard format. The documents are received, validated, and accepted into the job stream of the receiving computer, and immediately processed if so desired.

The format in EDI is governed by a predetermined set of rules known as standards. While the exchange is computer application to computer application, it is important to emphasize that this exchange of electronic business documents can take place between totally different systems environments, with very different equipment hardware, operating systems, and applications. It is precisely in order to satisfy those constraints associated with differing environments, that EDI becomes the coupling link allowing application to application transfer of documents. Therefore, in this sense a true EDI standard protocol, is both hardware and software independent.

The foregoing definition is possibly the most general definition of EDI imaginable. There are however, other means of electronic transmission which do not involve standard formats, or necessarily computer to computer exchanges in terms of computer application job streams. Those are generally referred to as other Electronic Commerce (EC) technologies. Examples of this would be, using a FAX to order goods, dialing or keying in orders, processing interdepartmental documents in proprietary formats, or various forms of electronic mail. These transactions are not considered to be EDI.

<table>
<thead>
<tr>
<th>EDI Is</th>
<th>EDI Is Not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer application to computer application exchange of business documents in a public or industry standard format using communications link between economic trading partners. Examples are: Requests for quotation Purchase Orders Invoices Payment Orders</td>
<td>Free format, electronic data transmission such as: Public E-mail — Internet Electronic mail FAX messages Text document exchange Videotext Processing documents using proprietary formats Dialing or keying in transactions Bar Coding Bulletin Board (BBS) Magnetic tapes</td>
</tr>
</tbody>
</table>
The EDI infrastructure is composed of three main components.

- A standard message format
- Translation software
- Communication network

Standards are the common language spoken when dealing with trading partners. A standard has to be a generic, comprehensive protocol, agreed to by a sufficiently wide group of user corporations. This is the case when you consider American National Standards Institute (ANSI) X12 as being just such a standard, sometimes referred to as a public standard. Standards also applies to industry-specific protocols. A few examples of those are:

- Transportation Data Coordinating Committee (TDCC) for the transportation industry.
- Uniform Communications Standards (UCS) for the grocery industry.
- Warehouse Industry Network Standards (WINS) for the warehousing industry.

A standard suggests that there is a dictionary which defines each message, component, element, and segment, of a data set, that users will comply with in order to exchange documents.

The translation software performs data conversion from the trading partners internal application format to the standard format in use. It is merely an interface layer specifically designed to convert the internal data and file format to the public standard format. Such translation softwares have been developed by vendors to satisfy an extremely wide variety of internal formats. It is important to appreciate that what becomes the key here, is that such vendors continually maintain their software releases to meet the most current changes enacted by the agencies overseeing standards pronouncements. Those are generally ASC of ANSI and EDIFACT. See page 5 for more on these standards.

Also, there is another point that can be made here regarding translation. The personal computer (PC) is the most widely used front-end platform for EDI use and all indications are that it will continue to be so. Further as a result of the evolution touching on the use of EDI many accounting software manufacturers have also included into their packages the added functionality of translation. That feature indeed does readily allow for data entry into the application by means other than the keyboard.

The component of communications provides information transport capabilities and other associated value-added services such as mailbox facilities, forwarding, and protocol-line speed conversion. What is commonly referred to as a value-added network (VAN) is simply a communications hub offering facilities for various services over and beyond simple communications. A VAN then can be thought of as a computing facility where the various EDI users can place EDI envelopes in mailboxes for trading partners which will be processed by them in due course and under their own respective schedules.
In the context of EDI where the basic object is to exchange documents between the trading partners, obviously first and foremost the documents themselves have to be generated by the sending party. Generally this involves the selection of data items from the database along with related messages to complete a specific document ready for translation to the public format. Take for example a purchase order. The preparation of a document represents three separate steps. Those steps are, mapping, data extraction, and the translation from environment-specific data format to generic format.

Mapping simply refers to the identification of those data items needed to fill out a particular EDI message as defined by the public standard format, in this case a purchase order, namely message 850 in ANSI ASC X12. You can think of mapping as though it is much like a spreadsheet, generally referred to as a two-dimensional flat file. Once these data items are identified, then they have to be extracted from the various data files, or database as the case may be, depending on the type of environment under consideration. Once these data items are assembled on a flat file, then the next step is the translation of the file to the actual public standard format, preparing it for transmission over the communications network.

In general terms, the relationship of the three EDI components can be represented schematically as follows:

In the appendix to this chapter there is an illustration depicting the actual structure of an EDI message format and the built-in controls using the ANSI ASC X12 standard code.
EDI Standard Formats

Just like everything else in an advanced economy, there have to be standards to which everyone rallies, thereby enhancing development and growth and reducing overall cost. We have seen that several industries have developed their own specific standards in order to address their own specific needs. At the time those industries were generating their own standards, that was surely a most welcome tool to serve industry members, facilitating transactions and so on. However, over time the need became evident that in some ways cross-industry standards had to be enacted. For example, think of a major railway which has to support three standards: TDCC because it is in transportation, X12 because it is in North America, and EDIFACT for European transactions. This adds cost, problems of logistics, and systems maintenance, making the whole process more incident prone, and obviously a less desirable situation than having a single overall comprehensive standard.

Accredited Standards Committee (ASC) of ANSI

The American National Standards Institute (ANSI), chartered an Accredited Standards Committee (ASC), whose mission it was to establish EDI standards that would cut across all industry segments. This came to be known as X12. ASC X12 updated and published all their standards. The Industry Standards Transition Subcommittee was formed to review the transaction sets of TDCC (Air, Motor, Ocean, and Rail) for compliance to X12 standards. Another subcommittee, Distribution and Warehousing, would review the transaction sets of UCC (UCS, WINS, and VICS). The ultimate objective pursued by the committees in respect of the terms of reference setting them up, was to emerge with one common, completely generic, fully comprehensive, public EDI Standard. X12 standards have evolved under a rigorous control process closely monitored by ANSI, which as opposed to industry formats made provision for adequate audit trails and controls as a significant added benefit. Another important benefit resulting from the ASC X12 effort is that the software vendor community could rely on a fully supported and continually evolutive and consistent standard, giving them an opportunity to include the necessary controls and audit features to their software offerings. While X12 is by far the pervasive North American standard format there is however yet another EDI standard format of very significant importance, namely UN/EDIFACT.

International Standards Development

UN/EDIFACT

The acronym stands for United Nations/EDI for Administration, Commerce, and Transport. This is mostly referred to by its common name EDIFACT. This is the adopted standard in many parts of the world and is expected to become the predominant standard for international EDI transactions. Clearly, it is easy to observe that one common international standard would be the best avenue to resolve international exchanges.

International commerce needs fast, efficient and accurate information to ensure the smooth flow of goods and services. EDIFACT has been developed as the specific solution to these universally recognized problems which ANSI also concurrently addresses. EDIFACT is the standard promoted by the United Nations for member nations.

EDIFACT has established five regional boards as advisors for international standards: Pan American, Western Europe, Eastern Europe, Japan/Singapore, and Australia/New Zealand. Each regional board has a Rapporteur to initiate and coordinate EDIFACT development work in their geographical area of jurisdiction. A Rapporteur is a person nominated by their government and appointed
by UN/ECE WP.4 (United Nations Economic Commission for Europe, subgroup/Working-Party 4 on Facilitation of International Trade Procedures). For more than 10 years, WP.4 has been developing standards covering data elements, codes, messages and syntax rules for EDI. The EDIFACT standards provide the world market with the necessary ingredients for applying EDI.

In Europe, the Western European EDIFACT Board consists of eight message development groups: Trade, Customs, Construction, Insurance, Transportation, Finance, Statistics, and Tourism. In the Americas, the Pan American EDIFACT Board (PAEB) serves as the coordinating body of Pan American national EDI standards organizations, and provides a forum for Pan American representation and consensus to the EDIFACT Rapporteur. EDIFACT standards development, maintenance and technical assessment in North America occurs within ASC X12 in the USA and the joint Canadian General Standards Board (CGSB) and Canadian Standards Association (CSA), Technical Committee on EDI (JTC/EDI) in Canada.9

One of the most well-known and widely used overseas standards is the Trade Data Interchange (TDI), used primarily in the European Economic Community for warehousing and distribution. TRADACOMS, developed in 1982 by the Article Number Association (ANA), is commonly used throughout the U.K. and
includes more than 20 documents across a wide variety of industries. Other standards include the Organization for Data Exchange Through Tele-Transmission in Europe (ODETTE), which is used in the European automobile industry, and Data Interchange for Shipping (DISH), used in European transportation industries.

With the existence of two prevalent standards in parallel, the reader may wonder what the future holds in store for ANSI and EDIFACT as EDI gains prominence in the global marketplace. As matters stand now, ANSI X12 is mature and relatively more stable than EDIFACT with recognized transaction sets covering many industry sectors. EDIFACT standards appear to be in a catch-up mode, but in recent years, have taken a great leap forward.

With the integration of the European Common Market, free trade agreements such as the Canadian–United States Free Trade Agreement, and NAFTA, the growth of international trade will further underscore the importance of one set of EDI international standards for global commerce.

**Standards Limitations**

Ideally there should be a single set of EDI standards covering all EDI message types. That set of standards is now emerging from the UN/EDIFACT Board. In the interim, as can be expected there are significant problems yet to be resolved.

Current users of generic and industry-specific standards, such as X12, used by many industrial segments in North America, Odette for the Pan-European motor industry, and Tradacoms for the UK retail and related industries, are experiencing problems in attempting to migrate to UN/EDIFACT. So it is fair to expect that other standards be used alongside EDIFACT for a number of years. Further, the development of EDIFACT standards has been too slow for many users, and there are gaps in the standards that will contribute to delay the migration process.

A significant event touching the standards has to do with the ANSI principals who conducted a survey within the industry membership and determined that some 70% are in favor of migrating towards one common standard for worldwide trade. The ultimate objective would be to establish EDIFACT as the common standard. In November 1992 the membership of Accredited Standards Committee (ASC) X12 voted to adopt EDIFACT syntax for EDI standards by 1997.10

**The Most Current Update on Standards**

Open EDI: The First Step in a Global Information Infrastructure

The announcement came from Concord California on January 27, 1995, through a press release from the International Working Committee.

"The ISO/IEC JTC1/SC30 International Standardization Committee, representing more than sixteen countries from Europe, Pan American, and Asia, announced the availability of a Reference Model for Open-EDI, which is the new framework for coordinating standards development. This reference Model is an alternative method to the traditional EDI standards development process that is slow and cumbersome. The committee has worked on this project for three years, and has reached its first goal of making this Reference Model available for worldwide review and ballot. Reaching this milestone allows the Open-EDI concept to be openly shared and standards to be established in a structured manner."

---

There are two main problems with EDI today, communications issues and semantics. Both of these issues hinder the process of a true open trading environment. Open-EDI addresses these problems because it is rule-based, open, and will provide a framework to enable businesses to work together electronically. It allows for national infrastructure efforts to be in harmony with each other. Open-EDI also enables interworking among organizations through interoperability among EDI platforms, value-added services, network providers and user applications. Standardized dialogues exchanging standardized units of data, readily available for use, will open the electronic marketplace to wider participation by all users. All of the units of data will be registered as public information. Generic rules will enable users to formally specify the roles of the enterprises involved in Open-EDI and the expected behaviors as seen by their trading partners.

The SC30 committee is moving ahead to translate business needs into requirements for standardized tools that will facilitate business process reengineering (BPR) related to information exchange.

A great deal has been accomplished lately regarding standards. So, what follows attempts to provide a quick capsule on that progress for the benefit of the reader.

The ASC X12 Committee submitted a draft dated October 2, 1994, to the membership for approval at the January 1995, Concord, California meeting. The draft titled Plan for Technical Migration to, and Administrative Alignment with UN/EDIFACT, was in effect voted on and approved by the X12 committee membership.

The approved document sets the stage and provides a framework under which ASC X12 will adopt UN/EDIFACT as a single standard after the release of Version 4 of the American National Standards (ANS) which is expected in 1997. In Part A, General Statement it is said that ASC X12 will provide a process to enable ASC X12 Subcommittees to incorporate needed business functionality in X12 into UN/EDIFACT standards. Also that after the release of Version 4, ASC X12 will continue for a period of time, in accordance with the approved plan, to develop, maintain, approve and publish X12 syntax-based transaction sets and supporting documents, however, they shall not be submitted to ANSI for processing as ANS.

The pace of the migration is a function of certain critical success factors. Generally, those factors are held to be as follows:

- Approval of equivalent X12 business functionality in UN/EDIFACT;
- Speed at which X12 subcommittees accomplish their migration work;
- A binary data solution in UN/EDIFACT;
- Establishment of a UN/EDIFACT policy allowing National Messages;
- Harmonization of national and international EDI meeting schedules;
- Use of UN/EDIFACT by the EDI community;
- A responsive UN/EDIFACT administrative process;
- Timely and accurate publication of UN/EDIFACT documentation.

By 1997, the current Version 3 of the X12 ANS will be five years old and according to ASC X12 and ANSI procedures, it must be revised, reaffirmed, or withdrawn. Therefore, the contents of Release 3070 of the ASC X12 draft standards shall be the last release approved prior to, and form the basis of, the Version 4 syntax-based ANS.
The migration plan also states that data maintenance on existing X12 transaction sets and supporting documents shall continue as long as justified by reasonable business needs. After Release 3070, only corrective maintenance or essential enhancement shall be allowed to syntax, control structures, and security transaction sets.

As a last and pragmatic point, the plan states that prior to terminating all new transaction set development in X12 syntax, input and guidance from the EDI community shall be obtained by a survey to be conducted in 1997.

**Growth of EDI Technology**

EDI technology is not entirely new, but its acceptance by many industry segments as a viable business solution is relatively recent and growing rather fast. Discussions on the subject started back in 1968. The development and publication of the first set of standards took place in 1975. The business environment and the technological environment have changed considerably since, and just like even the smallest business operations are equipped with a telephone, a FAX machine and a PC, then it will be just as common for enterprises to be users of EDI as an application of technology. With the availability of most of the off-the-shelf EDI software packages on PCs, this technology now becomes easily accessible to a much wider spectrum of organizations irrespective of size and economic means.

In the USA, Canada and elsewhere, adding trading partners is only one source of growth in the EDI market. Another important source is from the conversion of non-EDI documents into standardized format, thus moving from FAX or data entry to full-blown EDI. In 1990, the EDI industry reported a revenue increase of 40% over the previous year. A recent survey demonstrates that the growth in Canada should maintain a rate of 25% to 30% a year for several years. The survey reports that EDI is used for a wide range of transactions, the most common of which is the purchase order (80% of respondents), invoicing (42%), transportation documents (25%) and financial (6%). Financial EDI will be a substantial contributor to the growth.

Hence, it is not too speculative to suggest that competitive pressures would eventually make EDI the preferred means for exchanging business documents. These organizations which can master this technology would be at a significant economic and competitive advantage over those which do not.

**Trends in Software and Hardware Usage**

On the basis of 13,000 interviews conducted between 1988 and 1991, by the EDI Group Ltd., the following interesting information was obtained regarding both the software and platforms used. The survey showed that the PC is the platform of choice for actual translation from environment-specific format to public format. Actually the mainframe is not far behind. The statistics demonstrate that the PC is involved in 59.1% of cases, and 54.7% for mainframes, while the midrange is 21.0%. Further the survey showed that the vast majority of users actually purchased off-the-shelf translation software, as opposed to attempting to develop their own.
The strategic importance of EDI will grow as organizations learn to manage information as a critical sensitive asset and resource, not simply regarded as a mere cost of doing business. Advances in EDI technology offer managers opportunities to gain much wider and faster access to valuable information with fewer errors in processing and reduced bureaucratic delays associated with paper document shuffling and control. Managing EDI does require new ways of managing trading partner relationships in order to optimize the incremental value they are adding to the end products or services. Managers have to find new ways to ensure that the integrity, security and confidentiality of information is maintained between trading partners. New definitions of controls are needed, and managers must be able to advise their organizations on how to tap the benefits and control the risks associated with EDI. Subsequent chapters in this book describe the controls which should be considered by an organization using EDI or contemplating using EDI.

There is an increasing demand placed on internal auditors to perform as internal consultants on matters relating to control and technology. Management at different levels should make it a point to draw on this valuable resource where appropriate. In information systems management, proactivity can contribute to more effective and efficient operations, higher quality information for strategic support and lower costs. The notion of proactivity is not trivial. It represents a realistic anticipation of likely problems, and plan for effective corrective solutions, in cases where such problems would occur. Obviously, this includes sufficient adequate controls, and preprogrammed fallback positions should things go wrong. Hence, contingency management must be considered as an integral part of the planning and design, right up front, in both business processes and related support systems. In attempting to be proactive, it follows without saying that not all is equal, and consequently does imply a sound knowledge of the business environment and systems environment, including how events, risks, preparedness, and responses can be escalated, and prioritized.

As an internal consultant on control, the internal auditor requires appropriate reference material to deliver quality services. Since the internal information systems auditor is virtually the only dedicated resource specializing on controls in an automated environment, the auditor must be in a position to offer informed opinions and advice to management on the nature, type, and attributes regarding control that should be designed and built into this type of environment. The basic underlying objective is to ensure sufficient auditability to ultimately provide control assurance to senior management and other stakeholders.

EDI has been trickling down from larger business organizations to smaller suppliers. When a large business organization makes a policy decision regarding the use of EDI, and moves to inform its suppliers to be on EDI within a prespecified period of time or else "you no longer supply us," can be referred to as a topdown effect. These ripples around a large player is not to be minimized. Think of an entrepreneur who might have specifically come into business to supply a particular component product to one of the large corporations and how the smaller business concern can be placed in a difficult situation. The small operation suddenly faces the necessity to implement EDI to be allowed to stay in business, while in other circumstances it would never have entertained the idea. The benefit is not all that obvious when considering that it might represent very few transactions, perhaps the equivalent of less than half a dozen per month.
Horizontally, on the other hand, within an industry when EDI becomes the tool to provide fast efficient service to the customer base, then for the other industry members not on EDI the message is clear. You join the bandwagon or survival is definitely at stake. We can refer to this as a cluster effect, where industry members over a certain period of time have to rally to similar behavioral patterns and services.\textsuperscript{16}

New Dimensions for the External Auditor

There is no question that information technology has impacted everyone. Every functional area of management, and auditing of all types have been impacted by the advent of sophisticated systems. Consequently, coping constructively, including using the technology to advantage is the only really effective solution. In the case of EDI and associated paperless environments which over time are expected to become pervasive, will contribute to make it more difficult and critical for the auditor. The issue regarding the kinds of evidence and related quality of that evidence must be addressed.

Clearly times are changing, and different intervening professionals have various roles to play. Systems professionals, internal auditors, systems auditors, operational auditors, and financial auditors, individually have specific mandates and objectives, but when viewed together collectively, they should serve an overall objective of control assurance.

Organization of the Book

This book is functionally organized in two parts. \textit{Part One—The EDI Environment}, where descriptions and analyses of issues pertinent to the application of EDI technology are made. These issues are: the environment, management, security technology, controls, evaluation of packages, and legal issues in implementation. In \textit{Part Two—Auditing EDI}, the issues specific to the audit procedures are covered. This is followed by a selected bibliography of recent publications, a glossary of EDI terminology, and a table of acronyms and expressions used in this book and related literature.
1. The electronic envelope at the interchange level is a package containing one or more documents, such as purchase orders, invoice payments or other, grouped into functional applications. These transaction sets are composed of data elements which together are sometimes referred to as segments. This can be thought of as equivalent to a record in a database.

2. A functional group is one or more transaction sets of like nature exchanged between trading partners in a single transmission session. For example, a number of purchase orders would be assembled into a functional group.
3. A transaction set is one complete electronic document corresponding to a business transaction between partners, which is represented by a record in a database. It can be regarded as an electronic image representation of a business transaction.

4. There are headers and trailers on everything at each level to provide the basic control structure for EDI, containing the parameters critical to the acknowledgment of messages exchanged between partners.

5. The ANSI X12 Standard Code for Headers and Trailers as shown in the envelope are:

   ISA  Header Start Interchange
   IEA  Trailer End Interchange
   GS   Header Start Functional Group
   GE   Trailer End Functional Group
   ST   Header Start Detail Segment (Message)
   SE   Trailer End Detail Segment

   The control codes trigger the beginning or the end of an item, so there is a predetermined and controlled flow of data items.

**UN/EDIFACT**

The UN/EDIFACT standard provides control features in the headers and trailers of its interchange, functional group, and message envelopes similar to those found in ANSI. These are:

   UNB  Header Start Interchange
   UNZ  Trailer End Interchange
   UNG  Header Start Functional Group
   UNE  Trailer End Functional Group
   UNH  Header Start Message
   UNT  Trailer End Message

   The headers identify and specify the respective interchange, functional group or message, while the trailers serve as a completeness check on the corresponding envelope by means of total count and reference numbers.
EDI Allows Very Different Computing Environments to Exchange Documents

EDI Process

IBM — MVS/XA
CICS — DB2

DEC/VAX/VMS
ORACLE

Public Format
X.12, EDIFACT, or
Industry Format
TDCC, UCS, WINS

EDI Three Component Infrastructure

Sender
IBM/DB2
Application
Translation
EDI Format

Communications

Receiver
VAX/ORACLE
EDI Format
Translation
Application
Acknowledgments

The system of acknowledgments works the same way in ANSI as in UN/EDIFACT. It informs trading partners that a transaction has taken place. In case of disputes between trading partners, the acknowledgment may also support the existence of a transaction. Taking the X12 format as an example, each transaction set, otherwise known as “message” in UN/EDIFACT, includes an acknowledgment which is provided by the postal service only when the mail is registered. In an EDI transaction set, functional acknowledgments (FA) are used to inform the originating trading partner of the status of the transaction set upon receipt.

Basically, an FA is an acknowledgment sent to a trading partner to indicate that:

1. A document has been received;
2. The received document has met EDI syntax standards compliance tests and will be processed through the EDI interface phase;
3. Or, the received document has failed compliance testing, hence it will not be processed, or it will be only once subjected to further notification.

In this way, for instance, a buyer knows that the purchase order was received by the supplier, and that it has been accepted for processing, or it has been rejected and requires correction and retransmission. It is imperative that the functional acknowledgment be correctly interpreted by the sender of the related transaction.

<table>
<thead>
<tr>
<th>UN/EDIFACT Standards</th>
<th>Current Status for Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Status 2</td>
</tr>
<tr>
<td>Finance</td>
<td>8</td>
</tr>
<tr>
<td>Material Management</td>
<td>1</td>
</tr>
<tr>
<td>Procurement</td>
<td>3</td>
</tr>
<tr>
<td>Product Data</td>
<td>1</td>
</tr>
<tr>
<td>Transportation</td>
<td>10</td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td>5</td>
</tr>
<tr>
<td>Syntax</td>
<td></td>
</tr>
<tr>
<td>Construction</td>
<td>6</td>
</tr>
<tr>
<td>Travel, Tourism</td>
<td>1</td>
</tr>
<tr>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>28</strong></td>
</tr>
</tbody>
</table>

Source: Office of the Comptroller General, June 1993
Usually, there are two UN/EDIFACT publications per year, depending on the standards development schedule. The two releases reflect all the messages supporting directories at two implementable stages. Those are Status 2 and Status 1.

- A Status 2 message is approved by the United Nations as a formal recommendation, and registered as a UN Standard Message.
- A Status 1 message is approved by the United Nations for trial use.

In UN/EDIFACT, the version-release process takes place on a Status 1 Directory. All messages that are at Status 2 also appear on the Status 1 Directory, along with messages that have just recently moved from Status 0 to Status 1.

On the other hand, the new messages are the ones which are currently in the process of work and discussions by the interested parties, and the results will become conclusive at some future date. Only then, a status change is possible.
References


Part One:
The EDI Environment
Chapter 2. The EDI Environment and Business Opportunities

EDI History

Although EDI as an application of technology is not new, it might be of interest to become aware of some elements of the history leading up to the present. It is perhaps useful to have some notion regarding the emergence of EDI and how through time it found serious proponents to enhance its growth. So, a brief review of some of the historical components can help us understand its evolution and related opportunities for business development.

As in most fields of human endeavor, EDI has had its pioneers who were instrumental to its development, implementation, and popularization. A valuable source of information on this subject is *EDI Forum — The Journal of Electronic Data Interchange*.' The 1988 founding issue provides an excellent review of the history of EDI from a North American perspective.

In 1975, the concerted efforts of the Transportation Data Coordination Committee (TDCC) led to the publication of the first set of standards as EDI began to gather momentum. Ralph Notto, past President of EDI, Inc., highlights six significant events leading to the current period underlying the staying power of the early standards:

- Definition of the technology for processing EDI transmissions (1976–1977)
- The A.D. Little study of the feasibility of EDI in the food and grocery industry and the resultant standards and pilot project (1977–1982)
- Involvement of the American National Standards Institute (ANSI) and development of the ANSI X12 generic EDI standards (1978–1988)
- Formation of the Joint EDI (JEDI) Committee and the broad agreement reached for the revision of the EDI data element dictionary (1983–1984)
- Development of international EDI standards, EDI for administration, commerce and trade, EDIFACT (1985–1988)

In addition, the founding issue of *EDI Forum* cites the work of several pioneers from the transportation, drug, food, and railroad industries as major contributors to the EDI movement. It should also be noted, that since the time of that issue, the Canadian financial institutions have joined forces in a collective effort to define their role and involvement in financial EDI. Since that contribution broke new grounds in EDI, a brief description of the work of the Canadian Inter-Financial Institution EDI Committee, now commonly referred to as Inter*EDI is included.
The Transportation Industry

Joseph G. Carley Jr., Director of Operations for Programs and Systems for the TDCC in Washington, D.C. from 1973 to 1975, worked closely with Ed Guilbert, President of TDCC, to establish EDI as a cornerstone for significant change in methods for data communications.

The Drug Industry

Richard C. Cook, Director of Operations and Research for the National Wholesale Druggists Association (NWDA), headed an NWDA Committee that developed an automated order entry system for 443 drug wholesalers and suppliers. In all, 443 companies under the leadership of Richard Cook were implementing solutions to transaction errors and improvements in profitability.

The Food and Grocery Industry

George Klima, former director of Accounting Systems and Procedures for Super Valu chain stores, turned his firm into a showcase for the U.S. grocery industry's Uniform Communication Standard (UCS) program. The result was more than 1,400 vendors through 100 brokers and 200 manufacturers exchanged transaction data daily. This has been unmatched worldwide in terms of partnership and magnitude.

The Railroad Industry

John Nelson, along with associates at the Missouri Pacific Railroad, developed the concept of dividing the business document or transaction into logical segments and data elements. This concept became the basis for all EDI syntactic structure of ANSI X12 and EDIFACT.

International Trade

Don Trafford, currently Chairman of the EDIFACT West European Technical Assessment Group, led the UN/Economic Commission for Europe team, in 1984 that produced an EDI standard which was unanimously accepted by all European countries and became the basis for EDIFACT standards. He also made major contributions to the simplification of international trade procedures in the early 1970's.

Canadian Financial Institutions

Craig Ballance, EDI product manager at the Royal Bank of Canada, chaired the Canadian Inter-Financial Institutions EDI Committee (Inter*EDI), formed in 1989. This committee is responsible for establishing standards for financial institutions exchanging transactions with each other through EDI. Under the auspices of this committee, seven task force subcommittees were formed, namely, Security, Standards, Settlement and Timing, Audit, Legal, Volume, and Networks. Each committee delivered its own respective set of applicable EDI standards. These standards were fully sanctioned by the participating Canadian financial member institutions.3
The Canadian Payments Association (CPA)

The Canadian Payments Association has approved the Standards and Guidelines Applicable to EDI Transaction (CPA Standard 023) in November 1992. This set of standards and guidelines governs the exchange of EDI transactions between Canadian financial institutions which are direct and indirect members of the Canadian clearing system.

Benefits of EDI

As can be observed from the preceding overview, EDI was born from a driving desire to tap the benefits of technology and automation to the fullest extent possible. The current literature on the subject points to the advantages and benefits to be derived from this technology, when properly implemented and accompanied with sufficient adequate controls. The authors want to provide the reader with at least a minimal outline of these potential benefits so that one may be in a better position to evaluate whether some of these often quoted benefits indeed materialize once EDI becomes operational. Although very often an organization will go the route of EDI resulting from top-down and clusters effects, it is important to ensure that eventual net benefits accrue to the organization. As a case in point, this is an area where an auditor should conduct a post-installation review to examine all aspects of the EDI resource and provide some level of control assurance. This is treated later in this text.

In one of the most comprehensive surveys of EDI users and those planning to use EDI involving 1,094 firms by J. Hansen and N. Hill, the respondents were asked to express their reasons and rationale for using EDI. The results of this open-ended question are shown below:

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick response &amp; access to information</td>
<td>47.1</td>
</tr>
<tr>
<td>Cost efficiency</td>
<td>20.4</td>
</tr>
<tr>
<td>Customer’s request</td>
<td>19.2</td>
</tr>
<tr>
<td>Effect of EDI on paperwork</td>
<td>12.4</td>
</tr>
<tr>
<td>Accuracy</td>
<td>9.8</td>
</tr>
<tr>
<td>Better communications</td>
<td>5.7</td>
</tr>
<tr>
<td>Ease of processing for order entry</td>
<td>5.5</td>
</tr>
<tr>
<td>Aids in accounting and billing</td>
<td>5.5</td>
</tr>
<tr>
<td>Better customer service</td>
<td>5.5</td>
</tr>
<tr>
<td>Tracing shipments</td>
<td>4.9</td>
</tr>
<tr>
<td>Remain competitive</td>
<td>4.9</td>
</tr>
<tr>
<td>Industry standards</td>
<td>4.0</td>
</tr>
<tr>
<td>Convenience</td>
<td>4.0</td>
</tr>
<tr>
<td>Reduce manpower</td>
<td>3.7</td>
</tr>
<tr>
<td>Reduction in inventory</td>
<td>3.2</td>
</tr>
</tbody>
</table>
The table does not include responses mentioned 10 times or less. In the same survey, respondents were also asked to rate several possible EDI benefits on a five-point scale from 1 to 5, where one is least important and five is the most important. The results are shown below:

<table>
<thead>
<tr>
<th>Benefit Factor</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved customer service</td>
<td>4.29</td>
</tr>
<tr>
<td>Improved control of data</td>
<td>4.14</td>
</tr>
<tr>
<td>Reduced clerical error</td>
<td>3.97</td>
</tr>
<tr>
<td>Decreased administrative cost</td>
<td>3.71</td>
</tr>
<tr>
<td>Decreased inventory cost</td>
<td>3.35</td>
</tr>
<tr>
<td>Increased sales</td>
<td>3.25</td>
</tr>
<tr>
<td>Decreased manufacturing cost</td>
<td>2.75</td>
</tr>
</tbody>
</table>

The authors point out, that all of the advantages cited in the open-ended questions relate directly or indirectly to improved service, the benefit factor which received the highest rating.

With EDI, customer service improves and cost efficiencies are realized with the avoidance of paper manipulation and data reentry by the recipient partner organization. It logically follows that data entry errors are eliminated. Capturing or entering data remains the most labor intensive dimension of automation. Customer service improves with faster response to request for quotations, confirmations and other marketing services. Getting quotes from a larger number of suppliers is also facilitated. Being better able to disseminate product information and take orders through a wide EDI network can increase market penetration and distribution significantly.

A more recent survey on the implementation of EDI in Canada, reveals that a majority of the respondents believed that the most significant benefits were the reinforcement of ties with a business partner, improved customer service, reduction of errors and increased reliability of information. Conversely, the difficulties by rank were: trying to integrate EDI with computer applications, difficulty in understanding EDI technology, EDI user training and trading partner agreement (TPA). The survey results support the actual success factors relating to the implementation of EDI. Those are: a strong commitment and involvement by top management, appreciation of the technology, setting up a pilot project with a business partner already using EDI, excellent user training, and a quality EDI implementation team.

EDI also provides superior new facilities for management to reduce inventory levels and associated costs. As an example, the instantaneous availability of information allows for the implementation of just-in-time (JIT) reaching the production line only when needed. The cost of managing the logistics and support for accounts payable and accounts receivable functions can be materially reduced or perhaps even eliminated altogether. This is made more plausible once you con-
Consider that trading partners’ financial institutions can settle payments through EDI, which include the necessary supportive accounting and reconciling figures to vouch for specific transactions. An obvious byproduct spinning off from EDI is a reduction in the bank float. Payments are made directly between the trading partners’ bank accounts the moment the shipping notice is received electronically.

A shortened business cycle allows for cost savings and optimal management of operations. Trading entities have to appreciate the potential risks this technology can introduce and be vigilant in managing those risks prior to launching, and during the implementation of EDI.

Window of Opportunities

Although EDI had its beginnings in the U.S., it is gaining worldwide attention as a viable vehicle for international trade. The often-cited benefits such as faster response time and improved accuracy of information are equally applicable to global trading. In a December 1989 report on the subject of international EDI prepared by a California market research firm, the compelling reasons for using EDI elsewhere are the same: to reduce errors and to streamline the processing of trade documents involving numerous trading partners ranging from freight forwarders, brokers, banks, insurers, customs, to government agencies. As EDI begins to play an important role on the international scene, those organizations that have positioned themselves domestically will have a definite competitive edge linking up with new trading partners through common goals and business practices. Those organizations having mastered the correct technical infrastructure will find it a great deal easier to enter global markets.

In Canada the forecast for EDI is continued growth of 25% to 30% per year. Hence it is easy to foresee that EDI will impose itself as a business necessity both in North America and overseas. Business opportunities for EDI products and services in this industry, such as networks, payments, accounting, translation software, and consulting services are flourishing. There are reports suggesting that the removal of trade barriers in Europe is likely to cause an explosion in EDI. Vendors are now talking in terms of global trading partners management and global software.

EDI Gives Rise to Potential New Risks

More Interdependence and Increased Vulnerability

New applications of technology, while promising increased benefits, almost always carry potential new risks. This is particularly true given that the business objective with EDI is to enlist a large number of partners into a wide data communication network, to be used as a fully integrated tool to support transactions and business decisions.

With an increased number of partners, there is a corresponding increase in the level of interdependence upstream from suppliers and downstream to customers and clients. Technically speaking, EDI contributes to closer economic integration with trading partners. The domino effect of the mishaps of one partner within the EDI business cycle can make other trading partners vulnerable. Although the trading partner agreements can be relied upon to document each partner’s respective responsibilities and obligations, managers and auditors should have a heightened awareness of contingency planning and the additional risk reducing controls necessary to minimize risk to an acceptable tolerance.
Risks to Auditability

In non-EDI accounting information systems, paper based documents commonly referred to as source documents are used to capture information about transactions. Those documents become the original source for entries into the accounting records. Forms provide substantive evidence that transactions have been properly authorized and executed if signed or initialed by the persons responsible for authorization and execution. Also, forms are prenumbered so that it is easily determined whether transactions were inserted, deleted or processed more than once. Batch control totals and hash totals of grouped transactions are also used to check for addition, deletion or modification of transactions during input, processing and output.

EDI alters the traditional transaction audit trail, defined by the American Institute of Certified Public Accountants (AICPA) in Statement on Auditing Standards (SAS) No. 48, The Effect of Computer Processing on the Audit of Financial Statements, as a chain of evidence provided through coding, cross-references, and documentation connecting account balances and other summary results with original transactions and calculations.8 In many EDI systems, the complete audit trail useful for audit purposes may exist for only a short period of time and/or retained in a computer readable form. Without source documents and evidence of authorization such as signatures or initials, there is a risk that unauthorized persons might initiate transactions or modify the transaction trail. Automated controls involving electronic signatures, approvals, and authorizations should be designed and implemented to establish effective operational control. A not insignificant threat to auditability is the retention of records in magnetic media. If not well controlled, the result could be loss of data, or sometimes worse, contaminated data, which would severely hinder the auditability of EDI.

To date, most EDI applications have not involved the transmission of payments, the normal last step in a procurement cycle. This, in some respects has caused the deferral of the resolution of ensuring the integrity of electronic authorization for most EDI participants. Whenever EDI involves the electronic transmission of payments, there are several risks that must be addressed and controlled. These risks are particularly acute in EDI because of the trust which must be involved between the sender and the recipient of the payment transmission. The sender is placed in the position of having to rely on the recipient to have sufficient security and controls in place to ensure that the EDI transmission is not altered once received. Conversely the recipient depends on the sender to ensure that only mandated personnel are authorized to originate the transmission. Both parties have to count on each other to have sufficient controls in place to ensure that the messages transmitted are not read or altered by unauthorized persons. In the absence of a comprehensive system of data security, data could be subjected to unauthorized amendment or disclosure to third parties. This could result in additional cost from inaccurate processing, loss of competitive advantage leading to potential financial loss. Trading parties must trust one another that sufficient controls are implemented to ensure the accuracy and completeness of input, processing, and transmission of messages and actual transactions, to prevent errors or omissions leading to contingent losses.
The most critical risk in EDI payments systems is the mutual reliance between trading partners, if not well founded in objective and factual reality. Even with the best of intentions, certain trading parties may fail to implement or maintain adequate internal controls, thus exposing other trading parties to higher levels of uncontrolled risk. As discussed in Chapter 7, “Legal Issues in EDI Implementation,” the U.S. Internal Revenue Service (IRS) has introduced a provision requiring EDI users to establish the integrity of their EDI records. This in effect places the responsibility to demonstrate the integrity of the control environment squarely on the shoulders of the taxpayer corporation.

Risks of Third Party Network Providers

Using third party network providers to transmit EDI transactions to trading partners gives rise to a number of potential risks:

- Confidential information could be disclosed to unauthorized third parties, possibly even including competitors;
- Invalid and/or unauthorized transactions could be introduced by third party staff;
- One could be invoiced for services not rendered, either deliberately or erroneously;
- Transactions could be lost resulting from disruptions of data processing at third party network sites, or en route to the recipient partner, causing business losses, and inaccurate financial reporting;
- Audit trails could be lost when messages are passed from one network to another.

Application Failure

A review of the potential new risks related to EDI confirms that application failures or even systems downtime can have a significant negative effect on partners within the business cycle. The risk of failure of an application exposes the trading partners to potentially material losses unless effective contingency plans are in place to minimize the effect of an outage and allow fast recovery. This is made worse and more critical, where the EDI application is closely integrated with inventory management and production processing. In such situations the loss exposure is greater. Adequate contingency planning should include alternative methods for transmitting data, and if necessary, processing data. Management should also plan for recovering the EDI application, within the tolerance period from an outage, as derived from, and defined by appropriate impact and risk analyses. Specific controls for ensuring alternative processing and recoverability are discussed in Chapter 5.

Risks of Integration

Whenever within an EDI environment, information systems applications such as order processing become integrated with other business applications like accounting, issuance of payments, inventory management, and production control, the risk of a domino effect resulting from errors, omissions and failures is markedly increased. Large integrated systems such as those found in the life
insurance industry have been suffering the domino effect for many years. The speed of transactions and the lack of human intervention in EDI systems increases the magnitude of consequences several fold. Therefore, cost is proportionately higher, unless adequate compensating controls and contingency plans are implemented along with EDI.

There is also an important risk associated with the inability to master security technology like message authentication and data encryption. This aspect is described in Chapter 4.

Although readers might argue that paper-based and manual systems are exposed to serious risks, and that EDI is no more likely to suffer a breakdown in control and auditability than the systems it replaces, the high value and high degree of automation involved in EDI systems increases the potential loss exposure resulting from inadequate control planning and maintenance. Subsequent chapters provide a review of the controls necessary to manage these risks within an acceptable level of tolerance.
References

1. R.W. Notto, *EDI Standards — A Historical Perspective*, EDI FORUM, 1988, Founding Issue, p. 120. More pioneers were recognized in the 1989 issue.

2. Ibid, p. 96–103.

3. INTER*EDI, *Corporate-to-Financial Institution Control Guidelines*, Audit Task Force, Inter-Financial Institution EDI Committee. Two of the authors were leading members of this task force.


Chapter 3. Management Issues

This chapter addresses some of the key management issues which are of interest to business managers in these changing times. There is no question that EDI will play a major role in the way business transactions are conducted in the next several years. This will impact how the organization should structure to reduce risk, and enhance the chances for survival as a going concern.

Managing change is never an easy task, and the degree of difficulty is a function of the sources and types of pressures, placed on the management team. At this time in history, we seem to be moving out of a recession. The fact is, we are probably facing a restructuring economy, more than simply leaving the classic recession cycle. The information society will take its toll in terms of change, as we move from a mass production economy to a value-added economy. Almost nothing is guaranteed anymore, and a fresh approach must be enacted to effectively manage within this new business environment.

Far and away EDI is too important a subject for the going concern to abdicate it to the so-called techies. This is not meant in a demeaning sense. Rather, it suggests that the decision to go ahead with EDI is a policy decision that should be made at the highest level in the organization. The commitment and involvement should permeate the entire process of project management and implementation. Not all has yet been written and researched on this subject, but it is clear that line management and the business unit managers have to dominate and assume full managerial responsibility for EDI and related operational aspects.

Efficiency, Effectiveness, and Economy

Market competitiveness, administrative cost savings, accuracy and timeliness of information exchange and better quality control are the most frequently cited benefits of EDI. These attractive benefits are also the conditions necessary to fulfill the management objectives of efficiency, effectiveness, and economy, the three E’s.

At a time when markets are globalizing, and the economy is regionalizing as in the case of the North American Free Trade Agreement (NAFTA), it becomes obvious that efficiency and innovation are essential to both the competitiveness and the survival of an organization. Gaining the competitive edge is more than being the first entrant into the marketplace. Rather, it is the result of a sound corporate strategy, with commitment from senior management, the implementation, and execution of a properly thought out plan, continually reviewed, reassessed and readjusted. To be able to respond to change in a constructive manner requires, first to be well informed, and second to structure accordingly for effective action and results.

While administrative cost savings have been documented by many key EDI players, these savings could be wiped out by inadvertent loss of data during transmission, or the inability to master new controls such as authentication or inadequate trading partner relationship management.

In information management, the attributes of accuracy and timeliness are as important to managers as they are to auditors. Through the use of standard message formats and elimination of time-consuming data reentry, EDI can significantly reduce errors and shorten the processing between order and delivery, billing and settlement. One can therefore expect that information from EDI systems be more immediate and interactive as it consists of computer to computer exchange. Management should be cognizant of the fact that the exchange is at
the inter-organizational level. As the usage of EDI grows, it is likely that organizations will share a portion of their information with their trading partners either for business reasons or for expediency, resulting in inter-organizational data merge or simply shared databases. Then, the control implications for managers and auditors is bound to be far-reaching.

With respect to the benefit of better quality control offered by EDI, it can be noted that quality is never an accident, the result of fanciful nature, and spontaneous creation. Rather it has to be specifically engineered into each EDI application. Adequate controls over the integrity, authenticity, confidentiality, and timeliness of information exchange can contribute significantly to the overall quality of an EDI system. These controls are described in Chapter 5.

Information technology (IT) is an important pressure component on management. Information systems (IS) have become pervasive, and the going concern has come to completely depend on the performance and quality of such systems. In the case of EDI, it makes the overall situation that much more critical, given that now the door is open to the world. There are also all the other problems in attempting to manage the IS resource in a continually optimal way. Important variables like functionality of the applications, levels of integration, maintenance costs, and capacity to migrate to newer technology are of special significance to management. Clearly, an important component in this context is the human resource, not to be neglected.

So, the question arises, what should the objectives for IS/IT be? Ideally, the ultimate objectives for IS/IT within organizations should be along three concurrent dimensions:

- Strategic Support
- Control Assurance
- Cost/Effectiveness

This should provide a relatively exhaustive set of objectives to be met, ongoing and as simultaneously as possible. Operations and total quality management (TQM) are included as a subset of these three objectives taken together.

Therefore, in a large organization, implementing EDI as a stand-alone application, disconnected from the computer applications might not be the best long-term solution.

It has often been said that EDI will change the way business is conducted. At the macro level, the key issue seems to be the establishment of a good trading partner relationship, or more precisely, the implementation of intercompany effectiveness. This approach is drastically at odds with the classical model of management where each company takes an insular view of the other. Stepping out of the insular position to embrace trading partners as an integral part of the value chain requires a totally different mindset and style of management. Recognizing that companies can be only as good as their weakest partner, and that many interdependencies exist within the EDI business cycle, managers should establish a program to systematically implement intercompany effectiveness. Michael Hammer says, "EDI gets at the fundamental assumption that organizations have boundaries." This aspect is further elaborated in the section, "Managing Trading Partners" on page 35.
The underlying concept of EDI implies that a company cannot act alone. Therefore, cooperative management is treated as a given. Concerted trading partners must strive for a win-win arrangement where the historical distrust between customers and distributors is removed. In this context, we can view EDI as a means of facilitating intercompany synergy, communications, and effectiveness.

Internally, the change brought about by EDI is more fundamental. The basic issue is not EDI for EDI's sake, but rather EDI for what? The answer to this is short and simple. It is a new way of doing business and carrying out economic transactions. The new expression for it is Electronic Commerce. In order to tap fully on the benefits of mechanization, and be able to take advantage of technology, more specifically information technology, then management must reengineer the various business processes. In fact, this is so important that it is not an option. Many EDI project managers will fail if they view EDI as merely a new piece of software to replace existing documents. EDI as one of many facilitating technologies must become a part of an overall change in management strategy, otherwise as an independent implementation it will fail to achieve its alleged potential. Such a strategy touches on the key variables, namely the structure, people, and processes.

Business Process Reengineering (BPR)

The verb reengineer suggests done with intelligence and skills. In other words all the variables, parameters, constraints, and resources of a given situation, pertaining to an existing structure and associated business processes will be modified in such a way as to yield the optimal new structure and processes for substantially enhanced performance. Hence, by definition BPR cannot be mere guesswork, improvisation and/or short-term patchwork. Sound BPR should deliver substantial cost savings, while improving responsiveness to market forces. The underlying rationale of BPR is to obtain maximum benefit from mechanization.

Many times the issues of skills, orientation, and training are raised with the introduction of new technology, a new process, or a new system. In the case of EDI, the impact on accounting cycles and accounting functions warrant special attention. Traditional accounting control reports are time-based to coincide with the established accounting periods and preselected cutoff points. This business cycle is now compressed through computer to computer exchange, effectively eliminating the need for paper-based documents such as purchase orders, invoices, or checks, and associated traditional paper-based control reports.

Furthermore, when trading partners settle their accounts through a financial institution with EDI facilities, the functions relative to accounts receivable and accounts payable are greatly diminished. While EDI has the potential for improving corporate cash management as a result of more timely information, the value of some of the traditional accounting functions are significantly challenged. At the same time, management's ability to establish controls based on external sources are reduced. To prepare for this change, managers and auditors should focus on the manual or automated controls that EDI replaces, and examine how the proposed environment achieves the same result or better. It is expected that the added complexity and sophistication of new EDI systems will increase management's dependence on automated controls to monitor the EDI process in its entirety. This in turn requires tighter proactive control over systems development and related maintenance. Everyone in the organization interfacing with the EDI environment should be trained in EDI and given incentives to look for opportunities for EDI to enhance contribution to the strategic objectives.
Pilot Mode Caution

It is common practice for organizations to begin EDI in a pilot mode within a small local unit. Pilots make good business sense as risk associated with them is low, and the number of participants is few. If mistakes are made the consequences are not devastating and less costly. To a large extent pilots provide opportunities to develop trust and confidence levels with trading partners as well. We saw in Chapter 2, that a recent survey in Canada regarding success factors in EDI implementation, demonstrates the importance of setting up a pilot. However, managers and auditors should be aware that controls are usually more relaxed in pilot projects, which are usually run in a PC environment. Due to the short life expectancy of these systems and the disposable nature of the software, controls designed into pilot EDI projects may not be acceptable in full-blown, large-scale implementations. We recommend that project managers and auditors maintain a list of control weaknesses accepted in the pilot run and use it as a checklist at the starting point when evaluating controls required of the new environment.

Reorganization and Levels of Integration

Reorganization

Managing change entails the ability to anticipate what is to come. Once EDI is fully operational among trading partners across industry boundaries in a global context, the maturing of inter-enterprise systems or cooperative systems, now merely a concept, will be a reality. Reorganization will take place along either the distribution pipelines or value chains. The definition of a business concern may have to be reviewed and changed, since the interdependencies among the trading partners are so intricate that one can view the participants along the chain or pipeline as members of the same economic community. In fact, this is economic integration.

The present state of the art in EDI calls for computer to computer exchange of information, and it could be that EDI will eventually advance to full, direct application to application exchange. This would effectively eliminate the intermediate EDI flat file, trading partners have to use in order to communicate their business needs. G. Gerson, in his article on Data Mapping: The Integration of EDI into the Corporate Information Structure, sees five levels of integration from the paper system with no integration to full integration when EDI is used as the corporate interface mechanism. The control requirements for each level of integration are different. These are briefly discussed in Chapter 5.

Levels of Integration

Generally, there are three levels of EDI implementation, and each one relates to the level of integration with the actual computer business applications.

1. Pure stand-alone EDI
2. Application seamless integration (ASI)
3. Properly engineered business processes and paperless environments

The first one is a stand-alone computer like a PC or a midrange computer where inbound documents are received using the standard EDI format. Sometimes this is referred to as door-to-door EDI.

Conversely, the second is a much more sophisticated level whereby inbound documents are received, validated, and accepted into the job stream of the receiving computer applications.
Here attention must be paid to what can be described as the spread of EDI. In other words, what applications and/or what business functions are affected by EDI and what percentage. It could be that only a fraction of the functions are affected as in the case of dealing with only a few partners representing a portion of the procurement process or other function.

The third level can be described as full-blown EDI. In this category the business virtually deals with nobody not on EDI. In those environments, sourcing through EDI is a matter of corporate policy and no exceptions are allowed. The very organizational design is such that the actual business processes are fully engineered to take maximum benefits from mechanization. Those environments are virtually without paper, and many of the otherwise needed intermediate processes and steps are totally eliminated. Examples can be found in manufacturing where the concepts and principles of just-in-time (JIT) are applied, and quick response (QR) in distribution. Both are paperless environments.

So, we can surmise that EDI is all about integration. It is the degree of seamlessness achieved in incorporating information received into the business operation that is management's major preoccupation. As a matter of interest to managers and auditors, each progressive level of integration signals a higher level of complexity, sophistication, dependency, vulnerability, and contingency. Pre-verification of the controls added to each level of integration should be given special attention. Vigorous testing and auditors' early participation in the development process is strongly recommended.

Managing Trading Partners and Third Party Network Providers

Trading partners within the EDI business cycle are sometimes called members of the value chain. Value chains are linkages created with suppliers who furnish goods and services which add value to a company's product or service and delivers it to the customer. A value chain includes all of the goods and services from raw material to the finished product. It can be extended to include value added services provided by network suppliers and the paying agencies. The completed EDI business cycle is generally the incremental result of processes acting on materials, performed in a series by several companies.

Given the circumstances, the finished product of a business concern might be only as good as its worst trading partner within the chain. Recognizing this, many organizations are managing their value chains for competitive advantage. Digital Equipment Corporation recommends the following ten-step program, to effectively manage a value chain in order to optimize the value added:

1. Determine the critical trading partners within your value chain.
2. Analyze the actual flows of goods and services within the chain.
3. Determine the level of interdependence between the various members of your value chain.
4. Choose "good" partners: the critical ones who will benefit from your success to a significant degree.
5. Measure the level of efficiency and performance within your chain in terms of profit, cost structure, market share, service/quality/inventory levels, flexibility, growth rates and others.
6. Compare the above measures of your chain with those of competing chains.
7. Plan, in collaboration with your trading partners, the improvements of efficiency and performance levels.
EDI Control, Management, and Audit Issues

8. Define goals for improvements and implement them.
9. Monitor the improvement in these levels.
10. Plan for continuing improvement in these levels.

EDI is only one way for improving intercompany communications and effectiveness. Management should complete steps 1 to 7 before considering EDI. Understanding the way your partner conducts business is vital to enhancing partnership quality.

Managing Third Party Network Providers

EDI depends on numerous software and services supplied by third party network providers, consequently these relationships should be carefully managed to achieve optimal results:

1. During the evaluation of prospective network providers, among other considerations, request a copy of the auditor's report or third party review on the overall control assessment of the software or service to be provided.
2. Discuss with legal counsel regarding the "right to audit" clause in the vendor's agreement.
3. Details restricting the freedom of third party network to monitor the volume and direction of data traffic or to build statistical analysis out of it should be included in the third party network contract. Refer to Chapter 7 for details.
4. There should be regular meetings with third party network providers to review problems that occur to ensure that appropriate corrective actions have been taken. Such meetings should be chaired by senior management and attended by suppliers and managers responsible for these activities.
5. Availability of network and systems performance should be the subject of regular review especially in relation to the accuracy of billing statements and other records.
6. Review existing information security policy and communications policy with respect to an outside party to ensure that network security is addressed as a whole rather than piecemeal, taking into consideration all key controls and interactions external and internal to the organization.

Total Systems Dependence (TSD)

The advent of EDI and the generalization of its use, the associated economic integration with trading partners through the implementation of just-in-time (JIT) manufacturing and quick response in distribution, and the resulting paperless environments, all taken together represent, a complete dependence on systems. The downside is total paralysis should those systems fail, and the related adverse impacts on the going concern as an economic entity. TSD environments can sustain substantial losses if down even for a short period of time.

A Scenario

As a case in point, consider the following situation to illustrate the foregoing. Suppose a large retailer, with stores in numerous cities and towns across the country. The market strategy of that retailer is to be a large-scale discounting
operation selling brand-name consumer products, by skipping over the wholesaling distributor, dealing directly with manufacturers. Basically, one could think of an operation like this as a retailing hub for manufacturers. When this approach is combined with the high volume purchasing power of the retailer, the savings which can be passed on to the consumer through significant price reductions can indeed be substantial. In such situations competition cannot match the price differential if the operations and processes are not comparable. So these operations are like huge warehouse installations, geographically distributed in strategic locations, selling virtually anything the consumer might need. It is a one-stop shopping store with lots of parking space.

To make the strategy effective, the retailer signs contracts with manufacturers whereby a certain number of conditions are met to ensure advantageous pricing structures, smooth logistics, and avoid snags. Among those conditions you would find that EDI and Bar Coding are at the core of the arrangement. Further, the manufacturer does a portion of the management. An example, think of the manufacturer supplying paper products, like facial tissues, paper towels and so on. The manufacturer will make decisions regarding product mix, prices, quantities, when to ship, where to ship, and from which shipping point. The manufacturer is essentially managing a certain number of feet of linear shelves on behalf of the retailer.

When the goods come to the receiving door of the respective retail operation, the receiving staff simply captures the information using their code readers directly from the pallets’ wrap bar code labels or carton labels as the case may be. The information is relayed by radio frequency transmission directly into the computing environment and processed into the job stream as inventory. Depending on the approach used, there are situations where the manufacturer sends the information ahead of the shipment. When the shipment comes in and the code is read into the system it becomes the invoice and no further steps are required to validate the transaction which then gives rise to the payment process.

On the other side of the cycle, when the consumer does a purchase and goes through the cashier, more precisely called a point of sale (POS), the cashier passes the goods over the scanners to capture the pertinent data relative to each item purchased, right off the universal product code (UPC) which is on each product. That code defines all the information concerning the item.

The POS is a computer, serving as a front end to the host computer where the information relative to the sales operation is processed. There might be up to thirty or more POS stations hooked up to the same host in one physical location. This procedure credits sales for the various departments, reduces inventory, debits cash, or other debit accounts, like credit cards and trade receivables, generates the various management statistics for control and reporting purposes and any other associated control and management tasks which are designed into the system. Each transaction record is tagged by date, time, store number, POS operator code, and/or other record stamping desired. The POS is a sophisticated system handling many functions which are not nearly obvious to the consuming public, whose perception of the POS stations is as though they were mere cash registers. In fact, this is why the POS station is called cashier somewhat a misnomer. The combination of EDI, bar coding, and POS/UPC articulates a quick response to market demand in distribution.

Further, there are many other significant events taking place behind the scene. First, the retailer is sharing its data and information with the manufacturer which has access to the retailer’s computing environment through EDI. This allows for shared marketing management decisions not just the actual logistics. Second, the manufacturer must commit to and guarantee, fail-safe bar coding practices, and this is clearly spelled out in the contractual arrangement. Imagine
what would happen if the bar code was dysfunctional and the kinds of snags and mishaps this can cause. Third, how the logistics is controlled through a web of mechanical data capture and computing procedures, supporting the operations, but which also effectively supports the strategic plan of the business.

Again depending on the approach used, the accounting cycle is completed through EDI, whereby the manufacturer sends an electronic invoice to the retailer, and the retailer pays an electronic check to the manufacturer, financial institution to financial institution.

**Critical Issues**

There is plenty of material for one or more books on this type of operation alone, but for our purpose the foregoing is about enough to review a certain number of critical issues.

In terms of management practices this operation is at significant variance with classic paradigms of management. Clearly the business processes were engineered to take full benefit from mechanization. As a result paper disappears almost completely, giving rise to significant management trail and review issues.

What is even more significant is the fact that such an operation is totally systems dependent (TSD). This leads into the related issue of contingency and levels of assurance. Another significant difference from the past is the information sharing, and how the insular view is absent from the mindset. With respect to the above example, an economist would probably raise the issue of barriers to entry in the paper product market and/or retailing on a large scale.

The most critical issue from the management perspective is the total systems dependence to support operations and the strategic plan. While many times such dependence is achievable without EDI, the introduction of paperless transaction processing and procedures makes the entire situation a great deal more critical. From the accounting point of view, there is also total systems dependence to account for operations, and draw up financial statements. For auditors there are two levels of concern — the ability to raise the evidence necessary to support an opinion regarding the fairness of financial statements (this process is also totally systems dependent), and the monitoring required to control the environment on an ongoing basis throughout the period. The compliance aspect, and process control to provide control assurance is not exactly trivial, and does warrant special attention.

**Financial Statements**

The local host computers from the various stores across the nation are in communication with one central facility which provides management with instantaneous, accurate financial and operational information, throughout the organization. In a business of this type quite often the physical facilities are leased. Those leases tend to be pure operating leases. Consequently, the largest most significant asset is the inventory. Further, suppose that the retailer's contractual arrangement with some of the manufacturers is such that title is retained until sold to the ultimate consumer, much like a consignment situation. That indeed adds complexity to the operations.

The continued movement of inventory received and sold throughout the chain of stores, including the different triggers regarding title passage over the product mix, changes moment to moment. This is so complex that one must be able to lean fully on the systems to provide reliable information with respect to cutoff and valuation problems. In short, an instantaneous snapshot picture of the moving inventory asset is completely impossible outside the systems. This sce-
nario can be made as difficult and complicated as desired, like spanning several time zones, in a multinational environment, with currency translation and several other factors causing significant material impacts on the financial statements.

Control Assurance

Earlier it was suggested that control assurance be a concurrent objective for systems management. Control is a management responsibility forming an integral part of the mandate. Further management makes the policy decisions regarding the contingency, and levels of risk that the going concern can live with. Management has a free hand to make those decisions, and choose whatever rationale it feels appropriate under the circumstances to support the decisions regarding control. There are however, some conditions, call them constraints that must be met in order to insure impartial discharging of that mandate.

A first condition, perhaps the most obvious, is the accountability aspect of the management mandate. While management is responsible for control, the review and audit side represents the assurance aspect. The second condition is more intimately associated with the control objective, whereby sufficient, adequate controls must be in place to satisfy a number of stakeholding interests, in terms of compliance, contractual obligations, and other contingent responsibilities. The overall internal control system to safeguard the assets of the entity and insure compliance with the objectives and the plan of organization and related policies is also significant.

Within a TSD environment and EDI, management and perhaps even regulators should consider monitoring as a mandatory characteristic to be applied as a countervailing response to the systems dependency.

Monitoring, Control Data and Joint-Ownership

Monitoring

Generally, in computing environments there are three categories of software systems. Basic software, like operating systems, network managers, database managers, communications facilities and others are one category. Another category is represented by the various applications, like accounting, word processing, and other operational management functions software. The third category is the utilities, which are powerful pieces of software allowing the mandated users to accomplish certain tasks associated with maintenance, optimization, scheduling, extractions, report generating, or other systems management activities, allowing for a more secure and efficient computing environment. Within this generic category we find control software to manage libraries, change control, logical access control, and many other items of software.

What is not obvious in complex environments is the various layers involved. This is especially so, where applications are integrated into a seamless whole, over different platforms, using local area networks (LAN), wide area networks (WAN), gateways, and client/server systems. There might be many layers within a computing architecture, each representing its own level of complexity and significance for management and the auditor. Generally, those layers go all the way from physical to data, going through operating systems, interfaces and applications.

Basic software and control software, come equipped with two dimensions. The first one, is the reporting facilities available to the mandated user. The second dimension is the functionality command level where the mandated user executes various commands to perform optimizing tasks, or operate on certain parameters to enhance the computing environment according to changing situations and conditions.
Any reporting facilities available to management should also be available to the review and audit functions, internal and external. Monitoring systems should be part of the architectural design right up front, to satisfy the requirements of control assurance in TSD environments. Perhaps we can view this as a principle. Having equal access to such reporting facilities, does not exclude that the audit function have its own reporting facilities in the production environment where pertinent.

For example, embedded audit modules (EAMs) can be designed and implemented within the various critical applications. This is examined in more detail from a control perspective in Chapter 5. Such modules are native to an application and must follow the changes, enhancements and other maintenance interventions done to the application. Change control procedures have to be enacted to insure continued integrity. The advantage of the EAM is that the audit function has ownership of the module and related data it generates. Auditors are able to examine various aspects of the controls, do testing, change parameters, and raise evidence over the entire control period. A difficulty with EAMs is that they are application specific.

**Control Data and Joint-Ownership**

Monitoring data can be called control data on systems behavior, systems performance, and associated controls. A principle could be that both management and auditors have joint-responsibility of these systems and associated data. Effectively, this means joint-ownership. From this perspective management would not have a free hand to affect change to those systems without proper coordination with the auditing function. Refer to Chapter 5 for a discussion on monitoring systems and control on controls.

---

**Shift From Balance Sheet Focus to Operations**

The changes caused by technology, paperless environments, and the changed nature of the management trail, brings about the need for control assurance. This in turn gives rise to the need for monitoring, forcing focus on the entire control period, not just a point in time. The result is a shift in focus from balance sheet to operations. EDI/EC plays an important role affecting this change of focus. This is an indication of the expected changes to impact auditors in the next decade.

The operations and general business activities can be seen as a process. The balance sheet is simply the end position at a point in time, and valued according to generally accepted accounting principles (GAAP). For example, let us consider the difference between quality control versus quality assurance. Quality control is an event measuring the result of the process at the end when the product or output is finished. Conversely, quality assurance looks at the process and guarantees that the process behaves and performs as planned. If a business entity had its business processes control assured, then the balance sheet is simply the end result except for the valuation of certain balance sheet items.

**EDI Post-Installation Reviews**

Finally, management should not hesitate to seek an expert opinion regarding the EDI installation and operation. A thorough post-installation expert review should be conducted to examine all the key aspects of the installation and the operational management aspects of EDI. The results of the review, in terms of findings, observations, and recommendations can be very beneficial offering management a level of comfort and assurance.
References


4. Ibid.


14. The authors are indebted to Digital Equipment Corporation for this 10-step program on managing trading partners. This is by far the most practical method to date. In the USA, DEC uses EDI for nearly 80% of the procurement cycle, resulting in a 74% cost savings, and reducing the time cycle from 10 days to 3, with a redeployment of 30% of the related staff. Indeed, a true EDI success story.


EDI environments are characterized by three factors which coincide. Those factors are the disappearance of paper and related audit trail, high volumes at high speeds and the elimination of human intervention in transaction processing. This generally requires that managers and auditors consider particular security and control measures, depending on the nature of transactions and transmission. It is a prudent management practice to perform a risk analysis to examine the potential losses that can be associated with the messages to be transmitted by the proposed EDI system. This has to be done considering events whereby contents could be disclosed to unauthorized persons, or messages be accepted from dubious sources or altered during transmission. If the results of the analysis determine that authenticity of the originator or integrity of the message must be assured, management should consider the use of message authentication codes (MAC), often referred to as MACing.

On the other hand, if confidentiality of the messages is warranted, encryption should be seriously considered as a means of control. When these techniques are employed, managing the automated or manual key exchange between trading partners is a subject of prime importance. This chapter provides a basic understanding of the technology which can be employed to protect the integrity and confidentiality of EDI messages.

The ANSI Security Standards on message authentication, encryption and key management, represent the principal security control requirements in the inter-industry standards for EDI business documents. ANSI is the U.S. representative to the International Standards Organization (ISO). In early 1989, the ANSI committee, known as ASC X12, was mandated to develop such standards, and proposed two related technical standards for the security in EDI:

- X12.58 Security Structures
- X12.42 Cryptographic Service Message (CSM) Transaction Set

ANSI X12.58, defines data formats for security structures consisting of message authentication and encryption, following earlier ANSI standards X3.92 Data Encryption Algorithm (DEA), X3.106 Modes of Operation of the DEA, X9.23 Encryption of Wholesale Financial Messages, and X9.9 Financial Institution Message Authentication. ANSI X12.42 provides rules for the exchange of keying materials in an X12 environment based on the earlier standard X9.17 for key management. Where it is important to maintain the integrity and confidentiality of data to be transmitted, these message authentication and encryption standards should be considered in EDI technical systems specifications. ANSI supports the use of authentication and encryption independently or in combination. When both techniques are used, authentication should precede encryption for expediency purposes. The salient features of these techniques are discussed below.
EDI Security and Control Objectives

EDI implies trading partners and this could give rise to contingent liabilities of a significant nature or other material losses if not properly addressed in a proactive manner. This is made more acute when payments associated with financial EDI (FEDI) are part of the operations. Generally, there are six key threats that should be addressed in determining the attributes of EDI security and control. The security and controls supplied by most value added networks (VAN) are appreciably greater in terms of protection, than would typically be found in direct or point-to-point relationships.

Message Sequence Integrity

A message may be lost or replayed. There could be an accidental loss of a message or it could be replayed fraudulently. This feature requires that the receiver be able to identify data which is duplicated, skipped, or out-of-sequence.

Message Content Integrity

A message could be intercepted and modified. While maintaining a valid syntax a third party could modify a message to its advantage. Also, there could be accidental alteration and corruption of data while the syntax remains still valid. This attribute specifies that the receiver of an inbound message must be able to check that the data has not been altered.

Confidentiality of Message Content

Messages may be read by a third party. The objective is to avoid that any unauthorized third party gain access to the data and in so doing gain an unfair competitive advantage, or be in a position to impart harm to an organization resulting from the knowledge. This avoidance relates to situations equivalent to industrial espionage and/or financial gains resulting from lack of confidentiality. This attribute imposes on both the originator and receiver that they be able to guarantee that the data content is not subject to unauthorized disclosure.

Originator Authentication

This is non-repudiation of the origin. A sender might wish not to have sent a particular message and therefore later repudiates having done so. An obvious example is where a customer has ordered merchandise they no longer wish to receive and want to deny the responsibility or liability. The originator authentication requires that the recipient be able to verify that the originator is in fact the originator.

Recipient Authentication

This is non-repudiation of message receipt. The recipient may claim they never actually received a particular message. For example, a recipient might not have acted on a particular order and to avoid liability denies having received the message. Recipient authentication imposes that the demonstration can be made that the data was received and only received by the intended recipient.

Time or Timing Attribute

For this feature to be satisfied, the functionality must be able to demonstrate that the data and messages were delivered by a given time.
Message Authentication Code (MAC)

A Message Authentication Code (MAC) is a cryptographic check-sum value calculated by passing the entire message or authentication elements of the message through a cipher system. The sender attaches the MAC to the message before sending it. The receiver recalculates the MAC upon receipt and compares it with the sent MAC. If the two MACs are not equal, it is an indication that the message has been altered in some way during transmission, and the sender and receiver are alerted of the failure of the MAC code to authenticate the message. The objective of this technology is to insure integrity of the transmitted messages. If the information is altered the MAC would alert the receiver.

For EDI messages, authentication can also be used to detect attempts at deletion, duplication or insertion of messages. This can be accomplished by introducing unique identifiers, sequence numbers or date/time stamps into each EDI transaction. We can think of authentication much as though it is a form of electronic signature since it does identify the sender. Messages can still be in plain text form and readable by anyone being able to access the messages. In order to make messages totally unreadable by prospective unauthorized persons, encryption must be considered.

Encryption

Encryption is defined as the conversion of plaintext data into ciphertext data by using a cryptographic algorithm and key. Data are cryptographically disguised in such a way that only the parties with the key can view it in its native form. This cryptographic algorithm can be of many varieties, but the most widely accepted is the one generated according to the Data Encryption Standard (DES). Encryption protects the privacy of data passing between a sender and a receiver, irrespective of any communication nodes traversed by the message, as only the sender and the receiver are aware of the cryptographic key. However, the message source and destination identifiers must exist in plaintext form so that each node in the network knows how to route the message.

In ANSI, cryptographic security can be applied to different levels of an EDI transaction. It can be used to encrypt at the transaction level, for instance payment orders, or at a functional group level, batches of payment orders and purchases in one envelope, or both levels at the same time (see Appendix of Chapter 1). In EDI, transaction set level security is commonly used, since problems encountered at that lower level will not cause the entire functional group to be rejected.

Hardware Encryption

Hardware Security Modules (HSM) are self-contained, physically secure, special purpose computers that perform security-related processes and that securely store security-parameters and/or other sensitive data. These were developed when it was found that cryptographic processes could not be adequately protected under software control. Encryption performed by tamper-proof, physically secure hardware devices is far more secure than encryption performed by software. Typically, any unauthorized attempts to access an HSM results in its erasing of all sensitive security related data. They are also used to install cryptographic keys without disclosure to operators.
Security Key Management

When encryption and/or MACing techniques are used to secure EDI messages, maintaining the secrecy of keys is of critical importance. If unauthorized persons were to determine keys in clear text, they would be able to intercept, change and/or originate transactions without being detected. In the domain of automated key management, four main functions are involved. They are key definition, key generation, key distribution and key initialization.

Key Definition

The most common key management system is the data key scheme which involves three-level hierarchy of keys:

1. Master Key, also known as Master File Key:
   Unique to each network node and is used to protect keys or ciphers which are stored in a database.

2. Key Exchange Key (KEK):
   Unique to each link in the network. It is used to protect data keys in a secure manner during exchange between two nodes that are at the end points of a link. There are two encryption keys for each link in the network. The send key for one node is the receipt key for the other node, and vice versa.

3. Data Key, Working Key:
   Maintained for data encryption and message authentication. For each function, two data keys are maintained for each link in the network, for both the send and receive directions.

Key Generation

Keys are updated in two different modes. When the initial value of the key must be generated, it is done using a random number generation process. They are then installed in their respective nodes. Keys are updated in the following ways:

1. Master Key:
   Master keys are updated by generating and installing at each node a new randomly derived value. Key encryption keys must be decrypted under the old master key and then re-encrypted under the new master key. Such operations have no effect on other network nodes. This key is unique to each organization and should never be communicated outside of it.

2. Key Exchange Keys (KEK):
   The KEK must be developed in tandem between communicating partners by the exchange of key components to ensure that each KEK set is unique for that link. The node can initiate a KEK change. The node which does so produces a new key randomly generated and transmits it to the other node encrypted under the old key. After verifying its correctness, the receiving node overwrites the value of the previous key.

3. Data Keys:
   Each node determines the frequency of updating keys and sends them to the other node encrypted under the KEK.
Key Distribution

Keys are physically transported to the installation site for initialization. The principles of "dual custody with split knowledge" as stated in ANSI X9.17 should be respected. They may then be installed electronically using an HSM or if manually, they should be split into two parts so that two different persons can exercise control over each part without knowing the value of the other part. During key updates, the values can be electronically distributed. The custodians should not be selected from the application development area to ensure adequate segregation of duties.

Key Initialization

Once the two parts of the key have been entered into the terminal, the values of the initial KEK is computed and installs it in a key register or key pad linked to the HSM. The sender terminal then sends a message informing the other party's terminal so that key correspondence can be verified between the two. Upon installation, the key should be encrypted under the master key for the node.

Manual Key Exchange

To initiate an automated keying relationship, at least one KEK must be manually exchanged between trading partners. This involves several key exchange personnel who must carry out the key exchange function in a secure environment. Each financial institution communicates a key component which is exchanged and then combined to produce a key using an "exclusive or" (XOR) combination method. Trading partners should establish rules governing the administration and/or restriction on the use of keys amongst themselves. They should consult ANSI standards for the manner in which the keys are used.

The above is an overview of the security controls which can be applied to EDI. While the implementation of this technology rests with security specialists, managers and auditors should be cognizant of the essential features in order to properly manage the process, or to verify that such standards have been suitably applied in the EDI system under review.

Security Incident Reporting

This security control requirement, established by the Canadian Inter*EDI Financial Institutions for their own use, pertains to the reporting of security incidents, such as:

- Message authentication code verification failure
- Cryptographic service message counter out of sequence
- Known or suspected compromise during the manual key distribution process
- Known or suspected penetration of a physically secure device
- Known or suspected compromise of a key
- Key synchronization errors

This is further discussed in Chapter 5.
There are several security control aspects for managers and auditors to focus on. Obviously, the common objective is to pursue the most cost-effective security solution for EDI, be it MACing, encryption, or simply passwords and acknowledgments.

This chapter discusses the general features of MACing and encryption, the techniques of which are mainly used by financial institutions when transmitting payments-related messages. The security techniques described in this chapter are not the only methods available to ensure the integrity and confidentiality of messages. The level of protection required by an organization, should dictate the level of security to be applied. Other security techniques for confirming the authenticity of messages are available in this market to cater to the needs of various types of transactions and industries. These include passwords and acknowledgments, “challenge and response” added to dial access and digital signatures and so on. Another simple technique for protecting the confidentiality of a message is to break it into pieces and send each piece at a different time. However, the weaknesses inherent in these techniques should be well understood.

When considering EDI security, managers and auditors should be more concerned with message transmission than with stored information. The rationale behind this is that the level of protection on stored information is largely governed by asset value and the potential threats against that asset. With or without EDI, existing policies and procedures should be able to handle this aspect of EDI security. EDI messages entering into and leaving an organization is a new area that should be carefully examined. The controls surrounding EDI message transmission are further elaborated in Chapter 5.
References


Although most risks associated with EDI are similar in nature to those found in information systems and network systems, an evaluation of the controls in EDI should start with an analysis of what makes EDI special and unique with respect to other systems in order to obtain the right focus. The potential new risks discussed in Chapter 2 provides the background for a description of the control techniques presented in this chapter.

While the legal profession will address EDI control concerns in the light of accountability and liability, the role of the auditor is to ensure that the perceived new risks are properly addressed and managed by officers charged with this responsibility. Whether it be EDI or other information systems, the control objectives and audit objectives will not change. Those remain: accuracy, completeness, security, auditability, timeliness, and recoverability. Ultimately the objective of auditing should be that of providing control assurance. It is true that the focus may vary depending on the type of EDI transactions and the environment they operate in. As a case in point, financial versus nonfinancial applications, and the computing platform such as PC versus mainframe or other.

In view of the high speed and anticipated high volumes coupled with little human intervention in a near-paperless environment, it is prudent for both management and auditors to concentrate on preventive controls rather than after-the-fact exception reporting and corrective procedures. To be proactive in this situation can pay off significant dividends. It is equally important to ensure that these controls are pre-verified to function as designed, bearing in mind that the consequences of deficient controls are more far-reaching than non-EDI systems. The potential control solutions for each of the above control objectives are described below.

### Accuracy and Completeness

**Control Objective**

Integrity controls should be part of the business specifications and design upfront and built into the EDI system to ensure that transactions processed at the application level and environmental level are accurate and complete.

**Control Techniques**

At the application level:

The following key controls over accuracy and completeness of an EDI transaction should be considered:

1. Syntactic checks should be performed to determine compliance with accepted industry or public standards. It should be noted that this type of checking is usually performed by the translation software, which at best will ensure syntactic correctness, the presence of acceptable value types and codes, and the compliance with the standards which have been used. This level of checking cannot guarantee that unreasonable or impossible values will not be released. Special editing at the application level (such as reasonableness check or limit check) is recommended.
2. Each trading partner should advise each other of special editing against data dictionary items during application level checking to effect appropriate acknowledgments. Additional translation may be necessary after syntactic checks are successfully performed. This is sometimes necessary to bring data items in line with the special requirements of the recipient’s computer systems.

3. Criteria for positive and negative acknowledgments should be satisfied at each stage of processing, with details to be worked out between trading partners in accordance with prudent business practices. Items critical to such acknowledgments should be subjected to special edits. Examples are unreasonable purchase orders or invoice values. Trading partners should notify each other of any unusual items encountered prior to further processing. Examples are null values, cancellations or duplicates. Triggers which cause internal processing to commence will heavily depend on the extent of application level checking. The purpose is to promptly identify problems or errors so that timely and effective decisions can be made, thus enhancing accountability and reducing the severity of problems compounded at a later stage.

4. Continuous process monitoring using techniques such as embedded audit modules (EAM) can assist in timely identification and resolution of critical problems as they occur. See later in this chapter for a discussion on EAM’s and Integrated Test Facilities (ITF).

5. Sequence numbers and transaction numbers should be checked for uniqueness and serial continuity. Date and time stamps are important elements in the authentication process in detecting duplications and retransmissions.

6. Embedded headers and trailers at interchange, functional group and transaction set level should be checked to ensure that they are matched and the correct batches are processed.

7. Batch totals should be established, with the number and value to transactions to be determined and mutually agreed upon by the trading partners. Where feasible, on-line reconciliation should be considered.

8. Reporting of irregularities should be timely in accordance with procedures established between trading partners. Consider keeping these records in an Error File pending clearance. Context sensitive help or alerts should be considered at critical processing points.

9. Error logging and incident reporting should be outlined in the trading partner agreement. Common procedures for the review of errors and inconsistencies should be established.

10. Audit trails or management trails should contain sufficient details to prove the existence and evidence of an obligation. This refers to the classical items such as date/time stamp, access information, operator-ID and terminal-ID attached to a transaction which is machine readable and can be produced on demand. The issue here, is not whether the information is electronically stored or paper-based, but whether it is retrievable and certified to be a true copy of the records kept. Consider keeping a copy of critical documents with a reputable third party service provider as official backup.
At the environmental level:

The control techniques listed above are mainly designed to prevent bad input, inadvertent processing of erroneous data and to facilitate timely reporting and review of exceptions. The environmental controls surrounding the EDI system cover the broader spectrum beyond the input, processing and output specific to each application. The key environmental control techniques are presented as follows:

1. The quality assurance and change control process of vendor supplied software should be reviewed. This will include areas of network upgrade, versions of translation software and application programs. Ensure that vendors provide adequate documentation and timely update and release.

2. There should be evidence of sufficient and adequate testing especially in areas of message acknowledgments by both sender and recipient; special editing features; security technology such as MACing and encryption if employed.

3. There should be segregation of duties between the functions responsible for initiating, authorizing, recording and reconciling EDI transactions, particularly where these are not automated and/or integrated with existing applications.

4. An agreement should be reached between trading partners with respect to the migration of new versions and the maintenance of existing version of standards to be followed. This will ensure that the responsibility and accountability for errors outside the control of each trading partner can be traced.

5. Translation/communication software should be virus free. Consider adding a virus protection clause in the legal contract or request vendors to provide reasonable assurance that such threats have been addressed.

6. Liability for errors should be well-defined in the trading partner agreement. For more detail see Chapter 7.

7. Obtain an audit report from the vendor's auditors for an independent opinion of the control environment of the external party. Obtain the right to audit the vendor's products and services periodically to provide additional assurance on the continued functioning of controls.

8. Check if the vendor is prepared to write the Confidentiality Guarantee and Statement of Reliability or Integrity clauses into the contract. Although no vendor will provide absolute guarantee, all reputable vendors are committed to honor their corporate announcements. Complementary to this topic there could be a statement of adequacy of EDI control, which is a management representation and an audit opinion, external or internal, confirming the continued operation of controls.
Authorization Controls

The following key controls should be in continuous operation to ensure that all EDI transactions are authorized:

1. Operator Identification Code
   Every operator of the EDI System should be uniquely identified by a valid pre-authorized user identification code (User-ID).

2. Operator Password
   Every operator of the EDI System should have a valid pre-authorized password in conjunction with user-ID.

3. Operator Profile
   An operator profile should be determined for every operator in the EDI system. The profile defines and limits what actions an operator will be permitted to initiate.
   The operator profile should be used to limit operator activity within the EDI system to only those functions which have been pre-authorized by supervisory management.

4. Trading Partner Identifier
   All requests to access the EDI system should be further validated by means of a company identifier code. This code serves to identify the company as an authorized trading partner.

5. Maintenance of User Access Variables
   Maintenance of the user access variables, user-ID, password, and so on should be the object of logging, including update, creation, and deletion, as well as the identity of the person performing the change.

6. Regular Changing of Passwords
   Passwords should be regularly changed in a manner consistent with security management practices.

Security

Control Objective

The objective of security control is to ensure that all EDI related software and data are adequately protected against unauthorized disclosure or change during storage or transmission; and that physical access to the premises and the equipment is restricted to authorized users. Ensure that the most cost-effective security solution is pursued.

Control Techniques

With EDI systems, sufficient attention should be given to the security of data in transit, either mailboxed with a third party network provider, or enroute to the trading partner. As EDI data leaves the corporate entity, it may not be subjected to the same security policy and procedures each trading partner may prefer to follow. Major differences in philosophy over security issues should be resolved between trading partners and be well-documented and understood. It is a basic requirement that EDI is at least as secure as registered mail.

1. The security control procedures should include AUTHORIZATION procedures which emphasize the validity of the company as an authorized trading partner in the current business relationship. Validity checking against trading partner directory or profile and evidence of such checking must be documented.
2. Depending on the type of EDI transaction and risk, consideration should be given to Message Authentication Coding (MACing) added to message transmission to detect attempts to intercept or alter messages that are being transmitted. To be effective, MACing should be installed “end-to-end” across the network, otherwise it is unreliable.

3. This section is applicable only if Encryption and MACing techniques are used:

   a) Where Encryption during transmission is warranted, hardware or software solutions should be evaluated and appropriate encryption techniques adopted. ANSI X3.92 requires that DES algorithm be used in codebook form. Hardware encryption is performed at the host facilities, since software encryption is exposed to core dumps.

   b) When Encryption and/or MACing techniques are used to secure EDI messages, the restrictions on the use of keys should be observed. These include random generation of key values and no duplicate use of the same key in more than one function. A given key can be used for encryption or authentication, but not both. Similarly, a key can be used at the functional or transaction set level, but not both.

   c) Keys should be exchanged using dual control and split knowledge such that each key custodian is only responsible for generating one component of the key. The security operator who is responsible for providing security access to the custodians should not have any key information. After selection of components, written records should be archived or destroyed. Backup components should be inventoried, and routinely updated when keys are replaced.

   d) Procedures should be in place to ensure that each step in the key exchange process is carried out correctly. This includes keeping key exchange records current, availability of designated backups, key personnel changes and documenting the key exchange process.

4. Security violation reporting with regards to incidents involving logical access controls and/or message authentication should be provided. Such reports should be reviewed according to prudent management practices followed by appropriate action. Employees should be encouraged to report known or suspected security weaknesses or concerns, and under no circumstances should they be exploited. Statistics on key behavior like synchronization errors, MAC failure rates and so on, should be monitored and investigated.

5. There should be documented security incident escalation procedures between trading partners. Trading partners should respond to security incidents with the degree of urgency that is appropriate to the perceived severity of the incidents. Trading partners should notify the other partner immediately if it is determined that a risk has arisen to that partner.

6. Locking devices over terminals, telecommunication closets and work areas should be secure. A permanent record of equipment and software (serial number, model description and location) should be maintained, and a repair and maintenance removal log of each unit.
Auditability

Control Objective
The objective of auditability may be stated as the maintenance of adequate audit trails with regard to transactions sets, and the ability to pre-verify and adequately monitor electronic authorization and integrity controls of EDI transactions.

Definition
Auditability can be defined as that which has the properties and characteristics of being auditable. It refers to an area which can be fully audited and be demonstrated and substantiated in the course of an independent expert review. Information is auditable in the context of modern information systems when it can be substantiated by tracing it to source documents which can be based on paper or paperless media, or when reliance can be placed upon pre-verified, certified, and continually monitored control processes.

Major Issues
In manual systems, only the first part of the above definition of auditability is generally recognized. The ability to trace backward through the system to identify the component source transactions affecting an application database item, and the ability to trace forward a transaction through various intermediate processes to the database item affected has remained an essential part of the objective of auditability in computerized systems. These abilities are important when it is determined that reliance cannot be placed upon just one or more controls.

The second part of this definition of auditability is the reliance upon pre-verified and certified monitored control processes. This aspect first became necessary in the era of computerized batch processing, when the sheer volume of transactions made substantive auditing methods uneconomical. Such pre-verification usually involved auditing around the computer, comparing the results of manual and computer calculations for a sample of transactions. At best, it involved reviewing reports of exceptional items produced by special audit report generators. This became possible with the introduction of statistical sampling methods which permitted substantiation of a small sample of transactions, tracing them back to original source documents. Such pre-verification of controls was generally done in an interim audit, before the year-end audit, in order to determine whether the auditor could rely on the system of internal controls, and if so, avoid too many costly substantive auditing procedures, which can involve substantiating all transactions or large samples. Pre-verification of controls rarely involved testing computerized controls directly through test decks or integrated test facilities (ITF), embedded audit modules (EAM) or dummy entities, largely because of the existence, in the batch processing environment, of compensating manual controls, such as review of errors listings, and procedures for manual authorization and reconciliation.2

For on-line, real-time processing environments, pre-verification of computerized controls must involve on-line real-time testing of controls. On-line testing is necessary for the auditor to be able to raise convincing evidence supporting an objective opinion regarding adequacy and functionality at the point in time of the test. In the case of EDI and paperless environments where transactions are authorized electronically, auditability should also include the ability to pre-verify controls involving the use of user identification codes, individual passwords, user authorization profiles, terminal source, and message authenticity.
Control Objective

Management should ensure that appropriate backup, retention and contingency plans are in place to minimize the domino effect of systems or transaction failure on existing systems or other trading partners along the EDI time line. Prompt action should be taken to mitigate the adverse effects of such occurrences. In the event that it becomes necessary to recover, the recovery should be accomplished within a mutually acceptable time frame.

Control Techniques

The potential risks in EDI as discussed in Chapter 2 underline the importance of timely recovery of systems outage and that of a failed transaction set.  

Recovery of a Systems Outage

1. The roles and responsibilities for recovery in the event of a communication line failure between trading partners and service providers should be well defined.
2. Alternate mechanisms for the transfer of EDI information should be documented and tested on a regular basis as agreed. Report on such undertakings should be available to concerned parties on request.
3. Corporate contingency plans should include an estimate of the time required for reconstruction of EDI transactions in addition to normal processing needs. This may entail a review of the current assumptions underlying the maximum period for which an outage can be tolerated. It is also necessary to prioritize all applications under the contingency protection plan so that the impact of EDI on other systems can be gauged.
4. The trading partner agreement should spell out the periodic interval required for each party to test the contingency plans. Evidence of such testing should be retained for an agreed period of time.
5. Consider reversibility as a criterion in the event of unsuccessful systems change. For example a new version of standard or new release of translation software introduced into the EDI environment. An estimate of the time required to back out as a result of the aborted change may provide good insights to users and computer support groups in planning for contingencies.
6. Ensure that compatible backup hardware is on-site or that management has obtained vendor assurance that hardware can be replaced within agreed-upon time frames.
7. Operating procedures should be in place and duly executed. The restart and recovery procedures should ensure continuity of processing without duplication or loss of data.
8. Backups of system software and EDI information transmitted and received should be maintained to assist in system recovery. The retention policy should allow for sufficient time for error correction and resolution of disputes.
9. The recovery of any outage should be followed by either a manual or system verification that all transactions are accounted for. It may be necessary for management to provide a statement of compliance to the counter party that this aspect has been duly complied with.
Recovery of a Failed Transaction Set

There are two aspects to the recovery of a failed transaction set: timeliness in obtaining the trace information and the turnaround response time as agreed to between the trading partners to resolve such requests. It is customary to place the burden on the receiving party to question the accuracy, completeness and trustworthiness of a transaction. To properly establish error recovery procedures at the transaction set level, the following control techniques are recommended:

1. The type and extent of tracing information to be provided by the sender in the event of nonreceipt or errors reported by the recipient should be specified. Whether tracing requests are accepted by telephone or in writing or FAX should also be specified.
2. Retention requirements should take into consideration that sufficient time for error correction and resolution of disputes is allowed.
3. Trading partners should agree to the type of incidents to be logged and reported, as well as the length of time required for any incident to remain on record.
4. Where feasible, trading partners should share guidelines for investigation of incidents and standard methods for rectifying such situations.
5. The requirements and conditions for reversal or backout of transactions if necessary should be well-defined.

Controls Surrounding Third Party Network Providers

In evaluating the products and services of a growing number of network service providers, special consideration should be given to the controls built into these networks to ensure transaction security and integrity during transmission and upon arrival at the mailbox. It is important to understand the strengths and weaknesses of the various network providers.

Many vendors provide automated controls in areas of recovery, protection against data loss and error checking. In addition, they should also provide assurance that these controls are adequately tested or pre-verified. Management and auditors will then confirm the continual operation of these controls in the production environment. Where feasible, a prospective user of EDI should obtain an independent expert opinion on the security and internal controls of the network service provider of their choice. Apart from the normal contract terms such as service level, rights and obligations, and schedule for clearing mailboxes, the third party network provider should also supply the following control tools or information:

- Provision of volume traffic in sufficient detail to permit investigation of transmission errors or data loss.
- Confirmation of the customer’s absolute right to data in case of disputes.
- Provision of continuous service in the event of a disaster. The security of hot sites for the mainframe, if provided, should be comparable to the existing operational environment. Backup PCs should be virus-free and stand-alone sterile units dedicated to EDI.
- Availability of a log of transactions for a specified period needed to arbitrate the settlement of disputes between trading partners. Specifications of the format of this log and the storage media would be useful.
- Description of resilience built into the network to withstand occasional transmission problems or transient failures.
- Maintaining confidentiality of trading partner information through both physical and logical security mechanisms.
- Checklist for adding and deleting trading partners.
- Service guarantees provided.
- Provision of emergency delivery, if required.
- Justification for billing.
- Timely follow-up of errors and inconsistencies.
- Independent audit opinion on the vendor.

**Special Control Considerations for Financial EDI**

In addition to the controls described in this chapter, financial EDI transactions, which take place in the last stage of the EDI time line, deserve special attention. Traditional Electronic Funds Transfer (EFT), while performing similar functions as a financial EDI transaction, carries very limited payments information. Financial EDI (FEDI), on the other hand, is information-driven, not funds-driven. It has the capability of moving both funds and remittance information concurrently for ease of reconciliation, and to evolve into a new world class corporate payment system.

At the option of the payer, the remittance information can be collected, analyzed and reported back to the payer as specified, thus compressing the reconciliation cycle and unloading some of the accounts payable functions. As EDI information is integrated with existing applications, and shared throughout the company, there is a great potential for corporate cash managers to expand their influence over the entire treasury function.

A 1991 survey conducted by the National Automated Clearing House Association (NACHA) reported an annualized growth rate of up to 80% for U.S. corporate EDI payments sent through the Automated Clearing House (ACH) network. Reports from the European banking community are equally encouraging.

In Canada, an independent industry initiative called the Inter-Financial Institution EDI Committee, now called Inter*EDI, working with the assistance of the Canadian Bankers Association, has established the ground rules for financial EDI. Although these rules only govern the direct participants in the Canadian financial community, the following are some of the generic controls applicable to all financial EDI:

- Clear definition of liability and responsibility for payment.
- Vetting of all critical parameters affecting the liability transfer, especially by the legal counsel.
- Bundling of payment transactions received and delivered for end of day reconciliation with trading partner.
- Extended edits to be agreed by trading partners performed outside of the translation software.
- Mandatory authentication to verify the origin and integrity of the transaction.
- Optional encryption of selected payments or all of the information.
- Possible creation of an audit transaction set in EDI to facilitate continuous process monitoring.

As for the auditors reviewing this area of EDI, we suggest that new audit techniques and approaches be employed to continuously monitor the funds and information transfer process in a realtime environment. The following control techniques are specially suitable for auditing EDI:
EDC Control, Management, and Audit Issues

- On-line programs monitoring critical stages of EDI processing.  
- Audit database consisting of electronic audit trail information evidencing the existence of a transaction.
- Embedded audit modules (EAM) to inform the internal auditor when key automated controls fail to function as intended, thus allowing the auditor to give an opinion regarding the management’s compliance with a set of control standards over an entire control period rather than just a point in time.

Differences Between Funds Transfer and Financial EDI

<table>
<thead>
<tr>
<th>EFT</th>
<th>FEDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Payment transaction</td>
<td>- Payment transaction</td>
</tr>
<tr>
<td>- Value transfer only</td>
<td>- Value + remittance transfer</td>
</tr>
<tr>
<td>- Funds driven</td>
<td>- Information driven</td>
</tr>
<tr>
<td>- Retail or corporate customers</td>
<td>- Corporate-oriented</td>
</tr>
<tr>
<td>- Interbank proprietary formats</td>
<td>- Public format: ASC ANSI X12 or UN/EDIFACT</td>
</tr>
<tr>
<td>(i.e., SWIFT, CHIPS, FEDWIRE, ACH, etc.)</td>
<td></td>
</tr>
<tr>
<td>- CPA-005 (Canada only)</td>
<td>- CPA-023 (Canada only)</td>
</tr>
</tbody>
</table>

While there are a few similarities between EFT and FEDI, there is only one key feature that sufficiently distinguishes these two forms of electronic payments. Unlike EFT, FEDI has the ability to carry the desired level of remittance information with payment, hence adding more options to corporate payments information processing, and consequently prompting auditors to look beyond the existing controls built into EFT.

Both EFT and FEDI carry the basic payment information which consists of payment amount, value date, payer and payee account numbers and their financial institutions (FIs), method of payment and transaction reference and so on. For the EFT message, this is the bulk of the payment record, but for FEDI, this is only one component information. Other possible information components in FEDI are remittance advice, credit advice, debit advice and information which can potentially facilitate balance reporting, accounts reconciliation and cash management. Depending on the level of sophistication among EDI-capable FIs and their clients, many of the traditional treasury, accounts receivable and accounts payable functions may be downsized accordingly. In the future, when EDI matures, we can expect full automation of these functions and their increased effectiveness, as a result of the likely integration of information from credit granting, determination of payment terms, delivery schedules, funds transfer to ultimate financial transaction reporting.
There are two public EDI standard formats which handle payment messages. An analysis of the current version of the ANSI ASC X12 and UN/EDIFACT payment message formats reveals similar objectives behind the construction of payment related information. The only visible difference between these two formats is the ANSI treatment of aggregate information in one transaction set, and the EDIFACT segmentation of the same information in several messages. In either approach, the same types of payment information can be captured, if so desired.

Although the ANSI standard is more stable and mature, the recent activities of the EDIFACT Joint Rapporteur Team suggested that EDIFACT is beginning to catch up. In September 1992, this team met in Oslo to discuss the use of multifunctional finance messages. The concept was agreed to by the participants, and a proposal is being prepared by the Pan American EDIFACT Board. Another concept discussed in that meeting is the need to have the remittance information section better tailored to the needs of the various industries. The current remittance information was designed mostly by the food and transportation industries. But today, industry groups like health services, construction or financial services may have different needs. The following is a high level comparison of the two formats:

<table>
<thead>
<tr>
<th>ASC X12 Version 3020</th>
<th>EDIFACT Status 91.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>820 Payment Order/Remittance Advice</td>
<td>PAYORD Payment order only</td>
</tr>
<tr>
<td></td>
<td>PAYEXT Payment order and Remittance advice</td>
</tr>
<tr>
<td></td>
<td>DEBADV Debit advice</td>
</tr>
<tr>
<td></td>
<td>CREADV Credit advice</td>
</tr>
<tr>
<td></td>
<td>CREEXT Credit and remittance information</td>
</tr>
<tr>
<td></td>
<td>REMADV Remittance advice only</td>
</tr>
</tbody>
</table>

When the ANSI 820 transaction set is used to carry strictly “payment order” information — in the beginning data segment for payment order or remittance advice (BPR) — and when the EDIFACT “PAYORD” message format is used to relay payment instructions only, it is arguably correct to say that FEDI is just another form of EFT, since both the BPR data segment and “PAYORD” carry basic funds transfer information which is also carried by other wire transfer mechanisms. Under these scenarios, FEDI is only a variation of EFT theme. Consequently, the risks and exposures of FEDI and EDI are similar.

In applying general EDI environmental controls and existing EFT controls, users should not have specific concerns regarding this limited use of FEDI. It should be noted that in both EFT and FEDI, there are definite criteria to be met before funds can change hands. In the case of EFT, successful authentication is mandatory, while in the ANSI world, the Canadian financial institutions (FI) have officially announced their position that a positive application level acknowledgment is the key requirement. With the exception of the “REMADV” message, there is also provision in EDIFACT for authentication in all the remaining five messages. The success or failure of authentication is stored in the “AUT” segment of these messages. It should be noted that the “REMADV” message is not a
finance message per se as it is exchanged between two corporate entities and does not carry any payment instruction. This label of “finance message” may come from the fact that in North America, both JTC/EDI Finance and X12 Finance Groups are the “owners” of the message. In Europe, the Trade Group “owns” it.

As mentioned earlier, the differentiating feature between EFT and FEDI resides in the information content of the latter. Therefore, the ability of FEDI to carry various forms of payment related information is a new area which deserves special attention, since it may affect many traditional accounts receivable, payable and cash management functions of an organization.

The Canadian FEDI Audit Trail

An example of the new control in the Canadian FEDI is the presence of an audit trail which logs the movement of the 820 or 824 transaction sets. A direct participant in the Canadian payments system is a clearing member of the Canadian Payments Association (CPA). The originating payer’s FI may or may not be a direct participant, but it must assign a trace number to the transaction set. As the 820 or 824 travels from one financial trading partner to the next, each FI must append a CPA-assigned code to this trace number to form a continuous payment audit trail. This comprehensive logging and referencing gives the user as well as the auditor evidence of the existence of an authentic transaction.

Similarly, the U.S. Uniform Commercial Code Article 4A places the onus on banks, FI’s, and corporations to prove the audit trail in electronic environments such as EDI. Should something go wrong with a transmission, the courts will assign liability according to the audit trail. The party that breaks the audit trail would be placed in an unfavorable position.
The above represents the positive features about this FEDI audit trail. There is, however, one issue which must be clearly understood. The addition of a trace number by the FI does indeed alter the message and therefore the modified 820 must be treated as a new message. It should be recognized that the 820 coming from the payer or FI, is not the same as the one going out to another FI or the actual payee. In the EDI context, these are two different messages with their own reference numbers, date of creation stamp and so on. In terms of the archival requirements, each one of these messages must be considered and tracked.

When this audit trail is used in conjunction with the available referencing provided by the translation software and communications software, there is ostensibly sufficient proof where the transaction begins and ends. Trends and statistical analysis can be performed on this data to provide information about the behavior of controls over the complete period under review. When similar databases are created by the trading partner, periodic comparison of key control information may strengthen the authenticity and integrity of the underlying transactions. Trading partners sharing views of the EDI environment would facilitate enhancement of control for mutual benefit and comfort. This approach is superior to simply relying on trading partners based on unfounded trust. Further, to ensure project team buy-in, auditors should participate early in the EDI development cycle to allow sufficient time for their views to be considered.

Monitoring Systems and Control on Controls

In environments which can be described as totally systems dependent (TSD), and virtually paperless, there is a need for control assurance. As seen in Chapter 3, control assurance is a concurrent objective for information systems management. Monitoring is clearly a management responsibility as it is part of the control structure of an organization.

To meet the objective of control assurance, there is a concern for auditors having to raise value-added evidence to demonstrate compliance over the entire control period, not just a point in time. A significant objective is to maintain financial audits cost-effectively, as well as reduce the inherent audit risk. In critical environments described as TSD, there is no way around systems no matter how much we dislike it. One must be able to lean on the systems fully and completely. The use of EDI and associated business behavior with technology, will force a shift from balance sheet focus to actual operations. Issues touching on operational support and contingency affecting the going concern, the quality of evidence, and inherent audit risk cannot be dissociated from the systems, and could be hardly overstated.

Various layers of control can be implemented to satisfy the objective of control assurance. A key point is that those controls have to be cost-effective. Further, sometimes changing technology provides better and cheaper ways to accomplish what was virtually prohibitive in a previous tech cycle. In TSD environments, monitoring systems can be a cost-effective approach to control assurance, when all costs are considered. For instance, the auditor can request that the audit trail and control information be stored in a separate audit database restricted for audit use. The medium used could be in the form of CD-ROM or WORM devices, capturing either image replicated data or selected items based on criteria according to each set of situation specific circumstances. Those criteria parameters are specified by the auditor. Some key monitoring systems are listed below.
Embedded Audit Modules (EAM)

EAMs are recommended for FEDI. The Corporate-to-FI Control Guidelines propose that EAMs be used to monitor the integrity of controls, detect and report to the auditor or other appropriate parties on the failure to perform as required. There should be no restriction as to the generality of use, but the guidelines are specific to integrity of control regarding the following areas:

- Message Authentication
- Encryption and Decryption
- Security Incident Reporting
- Accuracy and Completeness Controls
- Authorization and Access

From an operational point of view, auditors should be the owners of EAMs. To avoid problems of jurisdiction we could recommend joint ownership of EAMs. The audit committee which has oversight responsibility could be a co-owner, and executive management be the other. Intellectually, it would be preferable that each have their own respective tools and independent means, but it can be recognized that it makes economic sense without compromising control assurance that there be joint-ownership of the modules.

Executive management and the audit committee would closely coordinate events affecting EAMs with respect to internal and external auditors. Appropriate procedural mechanisms should be implemented to consider application enhancements and maintenance affecting controls within those applications having a ripple effect on the EAMs. Change control procedures would pay special attention to the integrity of EAMs ongoing which is a significant component of control assurance within the control period. In paperless environments changes to applications can be very critical with a higher level of risk, requiring compensating procedural controls. It might be better to review and reengineer the entire change control procedure to ensure a cost-effective approach to satisfy the constraints imposed by control assurance.

Integrated Test Facility (ITF)

An ITF where available represents an excellent way to test live data transactions actually processed in the production environment. Proper transaction tagging is necessary to do reversing adjusting entries to master files, or database. Auditors are able to perform ongoing tests to check and ensure application controls are operational. Comparison is made against expected results and conclusions drawn up. In such an environment, selecting and tagging EDI transactions can be done to provide the audit function with an independent avenue to raising the evidence necessary. This is contingent on the spread of EDI versus which applications are available within the ITF. So knowledge of the environment comes first. For example, it is conceivable that EDI transactions only cover a certain percentage of the procurement function, and other subsystems handle the rest.

We can see so far, that whether an ITF is involved or EAMs or both, the first represents changes to the data files, while the second represents changes to the application programs. Both are in the production environment, and should be subject to appropriate change control, be protected and isolated from unauthorized access and use.
Using EAMs auditors are in a position to declare what parameters to activate for monitoring purposes, change the pattern of surveillance at will according to pre-defined objectives, concerns, risks, or evidence required. As a first technique we find real-time notification, capturing events as they occur, an example cash disbursement made to a particular supplier or other account where fraud is suspected.

Tagging is another technique. It generates an extended record permitting the reporting of the processing steps followed by an application to incoming transactions, which in other circumstances would not be saved as information. This is often used in limit checks where on the basis of criteria by the auditor anything equal to or exceeding an amount is tagged and reported into a specific file for later examination and review. Many times this technique is used in combination with snapshot before images and after images of data files. This allows the raising of evidence regarding logic errors, giving rise to errors in master file data. So an image is made before a transaction, then again after, and the results are compared against expected targets.
Chapter 5 Appendix A: Useful Information

Copies of the ANSI X.12 Standards can be obtained from:

- EDI Support Services
  Washington Publishing
  P.O. Box 203
  Chardon, OH 44024-0203  Phone: (216) 286-6810

Other ANSI Standards can be obtained from:

- American National Standards Institute
  11 West 42nd Street
  New York, NY 10036  Phone: (212) 642-4900

- Standards Sales Branch
  Standards Council of Canada
  45 O’Connor, Suite 1200
  Ottawa, Ontario
  K1P 6N7  Phone: (613) 238-3222  Fax: (613) 995-4564

Corporate-to-Financial Institution Control Guidelines can be obtained from:

- Canadian Bankers Association
  The Exchange Tower, Suite 600
  2 First Canadian Place
  Toronto, Ontario

- EDI Council of Canada
  5401 Eglington West, Suite 203
  Etobicoke, Ontario
  M9C 5K6  Phone: (416) 621-7160  Fax: (416) 620-9175

EDI Payments-Capable Guidelines can be obtained from:

- The Bankers EDI Council NACHA
  607 Herndon Parkway, Suite 200
  Herndon, VA 22070  Phone: (703) 742-9190

CPA Standard 023 — Standards and Guidelines Applicable to EDI Transactions can be obtained from:

- Canadian Payments Association
  Planning and Standards Development
  1212-50 O’Connor
  Ottawa, Ontario
  K1P 6Z2
### Chapter 5 Appendix B: Summary Control Matrix for EDI

#### SUMMARY CONTROL MATRIX FOR EDI

<table>
<thead>
<tr>
<th>Perceived Risks to</th>
<th>Control Objective</th>
<th>Control Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Management and Organization</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| ■ New way of doing business | Management should assess the impact of EDI on the organization's existing control structure and ensure that potential new risks are properly managed. | ■ Project controls  
■ Co-operative systems management  
■ Sound business strategy and executive commitment  
■ Industry representation and participation  
■ Trading partner agreement and other contractual arrangements  
■ Managing third party network providers  
■ Compliance program  
■ Control self-assessment program |
| ■ Redefinition of a company | | |
| ■ Intercompany dependencies | | |
| ■ Level of integration | | |
| ■ Compressed business cycles | | |
| **2. Accuracy and Completeness** | | |
| ■ Inaccurate and inappropriate transactions | Integrity controls should be designed upfront into the EDI system to ensure that transactions are accurate, and complete at the interchange, functional group, and transaction set levels. | ■ Application Controls:  
■ Syntactic checks  
■ Special editing  
■ Criteria for positive and negative acknowledgments at all levels  
■ Reasonableness check  
■ Checks for: exception items null values, cancellations, uniqueness and serial continuity  
■ Error logging  
■ Reporting of irregularities  
■ Use of embedded audit modules  
■ Pre-verification of controls  
■ Special controls for financial EDI |
| ■ Loss, destruction or corruption of data | | |
| ■ Inadvertent processing of rejected transactions | | |
| ■ Transmission or transaction errors | | |
| ■ Incomplete standards or versions | | |
| ■ Transmission/data quality | | |
| ■ Missing data elements | | |

*Continued on next page.*
<table>
<thead>
<tr>
<th>Perceived Risks to</th>
<th>Control Objective</th>
<th>Control Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Accuracy and Completeness (cont'd)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental Controls:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Quality assurance and change control process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Evidence of adequate and sufficient testing of software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Segregation of duties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Agreement on migration of new version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Maintenance of existing or new hardware or software upgrades</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Adequate documentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Controls over third party network providers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Security

- Unauthorized transaction sets
- Improper use or disclosure of business information
- Loss of competitive advantage
- Differing philosophy on security between trading partners
- Intercompany sharing of information
- Not mastering new security techniques
- Unauthorized alteration of transaction data

To ensure that all EDI-related software and data are adequately protected against unauthorized disclosure or change during storage or transmission; that physical access is restricted; and that the most effective EDI security solution is pursued.

- Authorization procedures
- Transaction identification
- Transaction authentication
- Encryption
- Hardware security modules
- Automated and manual key management
- Security incident logging and reporting
- Locking devices
<table>
<thead>
<tr>
<th>Perceived Risks to Control Objective</th>
<th>Control Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4. Auditability</strong></td>
<td></td>
</tr>
<tr>
<td>■ Loss of paper audit trails</td>
<td>To maintain adequate audit trails with regard to transaction sets and the ability to pre-verify and adequately monitor electronic authorization controls and integrity controls.</td>
</tr>
<tr>
<td>■ Loss of audit trail in transit between one network to the next</td>
<td></td>
</tr>
<tr>
<td>■ Difficulty with manual verification</td>
<td></td>
</tr>
<tr>
<td>■ Displacement of manual controls</td>
<td></td>
</tr>
<tr>
<td>■ Limitations of auditing around the computer</td>
<td></td>
</tr>
<tr>
<td><strong>5. Timeliness and Recoverability</strong></td>
<td></td>
</tr>
<tr>
<td>■ Disruption/delays in processing or transmission</td>
<td>To ensure that appropriate backup, retention and contingency plans are in place to minimize the sliding scale effects of a systems outage or transaction failure on existing systems and other partners.</td>
</tr>
<tr>
<td>■ Increased dependence and increased vulnerability</td>
<td></td>
</tr>
<tr>
<td>■ Domino effect on trading partner</td>
<td>■ Roles and responsibilities among trading partners</td>
</tr>
<tr>
<td>■ Not observing turnaround time in responding or resolving requests for tracing or recovery information</td>
<td>■ Alternate mechanism for EDI information transfer</td>
</tr>
<tr>
<td></td>
<td>■ Corporate contingency plan</td>
</tr>
<tr>
<td></td>
<td>■ Reversibility criteria</td>
</tr>
<tr>
<td></td>
<td>■ Compatible hardware</td>
</tr>
<tr>
<td></td>
<td>■ Restart and recovery procedures</td>
</tr>
<tr>
<td></td>
<td>■ Backups of system software and transmitted EDI information</td>
</tr>
<tr>
<td></td>
<td><strong>Recovery of a Failed Transaction Set:</strong></td>
</tr>
<tr>
<td></td>
<td>■ Retention requirements</td>
</tr>
<tr>
<td></td>
<td>■ Incidents to be logged</td>
</tr>
<tr>
<td></td>
<td>■ Sharing of guidelines between partners</td>
</tr>
</tbody>
</table>
References


3. The authors would like to acknowledge the contribution of Fritz Hildebrand and Terry Lawrence, members of the Canadian Inter-Financial Institution EDI Audit Task Force, Toronto, for some of the control techniques presented in this section.


Chapter 6.  

**Project Management and Package Evaluation**

From a broad-based perspective, managing an EDI project is no different from managing any major application system under development. So, it is expected that project risks are assessed, development methodologies followed, and project controls exercised to effect an orderly process and smooth progression towards implementation. This chapter does not elaborate on project management issues which are common to all large-scale development projects, but rather, the new areas of control and concern highlighted from the point of view of the project manager and the user coordinator. Further, the expanded role of the information systems auditor as an internal control consultant in proactive and cooperative mode with the project team, is illustrated.

**The Emergence of Inter-Enterprise Systems**

In a report published by Gartner Group Inc. on EDI software and services vendor evaluation, EDI is seen as a tool to develop inter-enterprise systems that are likely to introduce fundamental changes, not just in the way a company operates, but in the very definition of the company itself. Inter-enterprise systems require that the project team work closely with the systems' user personnel from other organizations to form a development platform serving as the basis for joint systems and project management for the best interest of all parties concerned.

Also known as *cooperative systems*, this concept has far reaching implications for project managers who must now look beyond the traditional systems boundaries of their own organization. As such, EDI project management will have to search for solutions serving all partners concerned, recognizing that any EDI system is as good as its weakest link. In dealing with various participating project groups, such as developers, MIS representatives, users and general business unit line management, each group is expanded to work with the trading partner's counterpart. Accordingly, EDI project controls must include proper relationship management with the project team from the trading partner organizations. The appointment of EDI coordinators or representatives from both the business and systems areas is seen as one of the important success variables in EDI implementation.

**Implementation Issues**

Some of the frequently cited roadblocks during the life cycle of an EDI project provide ample insights for project managers that such barriers must be removed or given considerable attention before an EDI project is launched. These implementation impediments include:

- Lack of strategic perspective;
- Absence of senior management commitment;
- Differing levels of sophistication among trading partners;
- Failure to integrate EDI into existing application systems and operations within an organization;
- Fragmented marketing of EDI to management and potential users.
Until these hurdles are overcome, EDI implementation phase will be pro­longed and the expected benefits will not be realized. To ensure a winning EDI implementation, project managers have to concentrate on the new implementa­tion issues attendant on this technology, such as:

- Focus on business strategy, not just on EDI as a system with promising fea­tures or functions;
- Treat EDI first and foremost as a product, or even better, as an extension of a product line, not a system;
- Look into the marketing, financial and organizational dimensions of EDI;
- Relationship building with trading partners;
- Executive commitment, management acceptance and employee buy-in;
- Potential organization-wide benefits when merged with existing information systems;

A close look at the above issues confirm that the success of any software develop­ment hinges on the management function. This fact is well summarized in an article in COMPUTERWORLD on this very subject. The lessons to be learned from some of the most effective software developers are worth citing:

1. Shoot for Effectiveness
   Distinguish working smarter from working faster. In the context of EDI, exploring and sharing options with the trading partners' counterparts is a good starting point. This is truly an example of a cooperative system aiming at a win-win solution.

2. Building Strong Platforms
   In addition to the implementation focus mentioned above, a coherent product plan, well-structured software architecture and anticipatory technology are equally important. The latter aspect, anticipatory technology, is especially relevant to EDI, considering the evolving national and global standards, while moving away from homegrown software to packaged software.

3. Make Effective Communications a Religion
   While effective communication is a given in systems development, this aspect is even more significant in cooperative systems where the project manager has to count on outside entities to provide a strong link to his or her own organization's EDI systems.

4. Foster Creativity
   In a disciplined framework, teams should be given freedom to find the best solution. In EDI systems development, it could mean transcending the corporate boundaries of an organization to tap into the resources and minds of the other team.
To add value to the project team, the information systems auditor must possess a broad-based perspective on EDI issues. Although as an application, EDI is a computer system, the auditor should first view EDI as a business strategy with potential for integrated application packaging crossing functional boundaries. The exchange of value-added information and communication may foster trading as well as information partnerships, but also underlines the need to establish guidelines for the exchange of specific information consistent with organizational policies.

During EDI development, an auditor can provide valuable service to the project team by focusing on the following items:

- Evidence of proactive planning versus reactive response;
- Existing manual controls that have been substituted with automated ones. The rule of thumb here is that the new controls must be at least as good as the old ones;
- Applying controls as appropriate to PC-based systems or mainframe EDI;
- Definition of responsibilities for maintaining versions of standards and trading partner directory;
- Cooperative problem solving and relationship-building with trading partners;
- Identification of qualified coordinator to deal competently with functional areas along the EDI time line, for example, marketing, purchasing, production, transportation, and finance;
- Industry affiliation and appropriate level of participation;
- Criteria for implementation sign-off by executives, if applicable, should include considerations which transcend organizational boundaries.

In the last few years, we have witnessed a growing number of EDI software vendors offering a wide range of products and services to prospective users of EDI. Not only are major computer companies such as IBM, Digital Equipment Corporation (DEC), General Electric Information Services (GEIS) in the market, and smaller firms are also trying to provide part of the EDI solution. It is anticipated that more users will purchase packaged EDI-capable applications and translation software than will develop home-grown proprietary EDI systems as a result of the maturing and acceptance of continental standards as in the case of ANSI, or international as in the case of UN/EDIFACT standards. The vendor selection process in this volatile market should be carefully examined.

The EDI market is populated with vendors offering products and services ranging from software and consulting to network. While most of the generic criteria for software package selection can be applied to EDI, the following are singled out for special attention:

- Current and future support of EDI standards;
- The standards approval process, concurrent number of generations supported, average lag time between standard adoption and software upgrade;
- Flexibility of communications support such as interfaces with leased lines and third party networks;
- Protocols from which translation is available;
EDI CONTROL, MANAGEMENT, AND AUDIT ISSUES

- Detailed description of the resilience built into the network/mailbox which has to withstand occasional transmission problems or transient failure of the network database;
- Details of guarantees provided to ensure message delivery and reporting capabilities in areas of success/failure of transmissions and the reporting security breaches;
- Mailbox facilities;
- Auditing of document life cycle;
- Mapping capabilities supported, flat file, on-line user defined interface or menu-driven;
- Upgradable from micro to mini or mainframe;
- Multiple hardware and software platforms supported;
- Security features, whether package can be used at a recovery site under comparable security;
- Availability of formal implementation plan;
- Details of archive facilities, on-line for short-term and off-line for long-term;
- External auditor’s report or independent review.

The above list highlights the areas that warrant both implementors’ and auditors’ attention, in addition to generic package selection checklists that can be found in most project manager’s handbooks as well as related audit programs.

Sources for More Vendor Information

For more information on the products and services provided by EDI vendors, the reader can consult the following publications. The details of these references can be found in the Bibliography section of this book:

References

Business messages between independent firms can have legal implications. Professionals must recognize, however, that legal issues are more important for some transactions than for others. Among the factors determining importance are the value of the particular transactions in question, whether they form contracts and whether particular government regulations apply to them.

Businesses use EDI to issue instructions to, and make commitments with, outside parties. EDI is often used to form legally binding contracts. An example of an EDI contract occurs when a buyer issues an EDI purchase order for 1,000 boxes of goods at $100 per box, and a seller responds with an affirmative EDI purchase order acknowledgment. The order is an "offer," the acknowledgment is an "acceptance" and together they constitute a contract. Both parties are legally required to buy and sell the 1,000 boxes at $100 per box.

Electronic contracts raise some issues: 1. Are they enforceable in court? 2. What terms and conditions are included within them? 3. Can they be proven in court? 4. How must they be recorded for tax purposes? 5. To what extent is a third party network liable if it loses an acceptance message and thereby prevents a contract from being formed?

A common method for addressing some of the legal issues in EDI is for each pair of trading partners to enter a Trading Partner Agreement (TPA). The American Bar Association has published a model EDI trading partner agreement (ABA Model). It is designed specifically for use with EDI purchase orders, although it can be modified for use with other documents, such as bills of lading and letters of credit. The hope is that the model agreement can help to standardize the trading partner agreements used in industry. This would save users time and trouble.

The ABA Model is only a model, not a mandatory standard. Users may modify its terms as they deem appropriate. Nevertheless, the Model offers a good place to start drafting an agreement, and gives an excellent checklist of issues.

The EDI Council of Canada has also published a model trading partner agreement, which is similar to the ABA Model. The choice whether or not to have a TPA is a business decision to be made by managers in consultation with their attorneys. The agreement can be analyzed in two parts:

A. terms dealing specifically with EDI communication, and
B. trade terms and conditions.

* Section I was written by Benjamin Wright, Attorney and Counselor, Dallas, Texas. © Copyright Benjamin Wright 1995.
Part A covers the manner in which EDI will be conducted, interpreted and enforced. Part B covers the underlying trade or "legal" terms and conditions that apply to the transaction effected through EDI, such as a purchase and sale. Parts A and B are discussed in more detail below. Despite the value of TPAs, they have a drawback. They can be time consuming to negotiate and sign. They require business people to enlist the attention of lawyers, and they can sometimes raise thorny, intractable issues. Accordingly, some EDI users can reasonably decide to forego TPAs, as the costs can appear to outweigh the benefits of the TPAs.

In addition, there are alternative measures, that fall short of full TPAs. A company could, for example, send a declaratory letter to its trading partner asserting the company's position and policy on the issues that would otherwise be in the TPA. Ideally the trading partner would sign this and return it, transforming it into a TPA. But there is a good chance the partner will not sign it. Still, the letter establishes the sender's position. In a dispute it may also give the sender an argument that its trading partner knew what the sender's terms were, did not object, and therefore implicitly agreed to those terms.

The Part A issues to the TPA include an agreement on whether EDI is considered "written," what will be considered a "signature" for EDI purposes, what communications standard (such as ANSI X12) the parties will use, what special modifications the parties will apply to the chosen standard, the division of liability in the event of an error or disaster, the requirement to maintain security and so on.

Perhaps the most critical issue in Part A deals with the writing and signing issues. There is some confusion whether EDI transactions are enforceable in court as contracts. The chief reason is that the "statute of frauds" generally requires some contracts to be supported by written and signed evidence to be enforceable. However, there seems to be consensus among knowledgeable lawyers that a well-drafted TPA can overcome this problem for all practical purposes.

How important is the writing/signing issue for a specific user? It depends. If the user is particularly concerned about the enforceability of its electronic contracts, the writing/signing issue deserves attention. If the value of these contracts is low, however, the issue may not be worth the time and expense it would take to deal with it. In addition, there is a persuasive argument that the statute of frauds as it stands today should consider recorded EDI contracts as enforceable even if the parties have no TPA.

Another issue is a determination of where messages have to be and when to have legal effect. Under the ABA Model, messages are not effective until they have reached a certain computer designated by the recipient. This issue is important, for example, if a company fixes a certain deadline each day after which messages will be rejected or will be processed at a more expensive rate.

The ABA Model contemplates that functional acknowledgment messages will always be used to confirm received messages. The Model's drafters felt that functional acknowledgments are so inexpensive that they should always be used. This could be a valid conclusion for many EDI implementations. However, the ABA Model was written by lawyers, not business managers. Some companies consider functional acknowledgments unnecessary. Alternative means for ensuring successful communication are available.

Some TPAs contain mutual trading partner obligations to acquire the equipment and services, and to institute the controls, necessary to conduct EDI securely and competently. The implication is that, if one partner fails to implement a good system, he must answer for any damages his partner suffers. This
mutual obligation may be appropriate in some instances, but it may not in others. Prior to EDI, parties did not agree to obtain the equipment and services necessary to open and respond to the mail. If a seller failed to open an envelope that contained a purchase order, the seller simply lost the order. But he was not legally liable to the buyer. The buyer knew that she could not rely on the order until she received a message from the seller accepting it.

It is prudent in more sophisticated EDI implementations to establish in the TPA norms for the sequencing of transactions. If it is contemplated that series of inter-related messages will be transmitted between trading partners (such as request for quotation, response to request, purchase order, purchase order acknowledgment, purchase order change, and so on), the TPA can describe and regulate the process. If the TPA is silent on the issue, there could be confusion as to precisely when obligations come into being as the result of an exchange of EDI messages. For example, after the exchange of a request for quotation and a response, is a purchase order all that is necessary to make a binding order, or must the buyer send a purchase order and wait for the seller to respond with an accepting purchase order acknowledgment? Some industries (such as the automotive industry) publish guidelines on these matters, which can be incorporated into a TPA. The ABA Model permits sequencing issues to be dealt with in the Model's Appendix, but the Model gives little guidance on what rules the parties should adopt.

Part B — Trade Terms and Conditions

Part B of the TPA deals with the trade terms and conditions (TT&Cs) that used to be printed on the backs of paper documents such as purchase orders and invoices.

Part B of the TPA is usually more important than Part A. Generally, it is much more likely that a serious dispute will arise out of the TT&Cs in Part B. They cover such issues as products liability for the goods sold via EDI, the policy for the return for defective goods and the warranty that the goods sold do not violate the patents of others.

EDI technology discourages communication of those terms in a fashion analogous to the way they were communicated in paper trading. The reason is that EDI standards are written for the communication of simple codes, not free-text legal clauses. Many companies — particularly sellers of goods — perceive the urgent need to affirm what they intend the TT&Cs to be in EDI. A user might take any number of approaches to TT&Cs — none is perfect.

One

The user can ignore TT&Cs. Then, if there were a dispute over terms, the law would apply terms by default. For example, suppose Supplier is selling equipment parts to Customer through EDI. They have no TPA and have not otherwise communicated TT&Cs. Some of the parts turn out a year later to be defective. Customer demands that Supplier replace the parts. Supplier refuses, saying that its policy is to warrant parts for only 90 days. Customer claims not to have known of, or agreed to, that warranty. It argues that the law automatically (by default) provides for a longer warranty. Customer would likely prevail. Article Two of the Uniform Commercial Code would furnish Customer a warranty that extends beyond 90 days.

A problem with the default terms is that they may not be exactly what the user wants. Another problem is that many believe the default terms provided by Uniform Commercial Code Article Two favor buyers over sellers.
Two

The user could reach an explicit but confused compromise with its trading partner using the following technique. The user and its partner would each attach its respective paper form (purchase order, acknowledgment or invoice) to the back of a TPA and then state in the TPA that the TT&Cs that shall govern each transaction will be those that would govern if the transaction had been effected with the use of the paper forms. This approach is not unusual in EDI. It gives parties (even sellers) a certain measure of comfort because it allows each party an opportunity to argue that its TT&Cs control over the other party's. This measure of comfort may be enough, depending on the value of the transactions involved. Yet this is an inelegant solution; it leaves the situation utterly ambiguous.

Three

The user could negotiate and agree with its trading partner on specific terms. This is the ideal alternative because it gives the greatest certainty. If the user already has a master purchase and sale agreement with its trading partner, then this alternative may be very easy to adopt. The user would just incorporate that master agreement into the TPA. If the user does not have a master agreement, however, negotiation of TT&Cs may be necessary, and negotiation is often time consuming. For many companies, this can be the greatest legal snag experienced in EDI implementation. Fortunately, one practicing attorney, Ralph M. Savage, has developed a form document to aid the negotiation process. It provides managers a checklist of major TT&Cs (for sales of goods transactions) so that they can negotiate the terms quickly.7

Four

The user could mail its trading partner a declaratory letter, as mentioned above.8 It would function much as a paper purchase order or purchase order acknowledgment does today. It would state the exclusive TT&Cs the user intends to do business under and invite the trading partner to sign it and return it. But it would declare that its terms control even if the trading partner does not sign and return it. The advantage of such a declaratory letter is that it is quick, avoids negotiation and in some cases may be effective in legally establishing the TT&Cs the sender desires. The disadvantage is that it may sometimes not be effective. But the form paper documents companies used before EDI suffered the same infirmity.

Finally

The user could engage in “electronic combat.” One large manufacturer has taken this position with each of its trading partners: It prefers that its trading partner sign a definitive agreement on TT&Cs. Yet if signing is delayed or refused, the manufacturer will continue exchanging EDI with that partner and will send its TT&Cs as an electronic message with each of its EDI transmissions. In effect, it breaks the informal rule that extensive free-text should not be communicated with EDI. It asserts its TT&Cs in a fashion similar to the way they were asserted before EDI — as writing on the backside of a paper form.

Some industry groups are drafting model agreements for their particular industries. These are tailored to cover industry-specific transactions. The Automotive Industry Action Group has issued a model agreement, which is based in large part on the ABA Model. Users should consult their own industry groups to see if they have special models.
EDI recordkeeping is important for several reasons. First, the parties need to be able to prove what they agreed to. Second, auditors need to be able to confirm transactions. Third, tax authorities need to see records of purchase orders, freight bills and invoices.

If there were a dispute between two trading partners over what they agreed to through EDI messages, the existence of evidence of the messages would be critical to any resolution. One can imagine Customer contending that its purchase order offered to buy 500 boxes and Supplier alleging the quantity was 1000.

To ascertain the truth, would a court consider any of the magnetic, optical or paper printout records maintained by the parties? One can imagine the opponent to such evidence arguing that it is too subject to error or fabrication to be useful in court. Magnetic records, for example, can be altered after-the-fact, without leaving a trace.

Judges, however, have been permitting the admission of computer records into courtroom evidence for over 20 years. The central question a judge wishes to know is whether the record is "reliable." There is some academic debate over the way in which judges ascertain the reliability of computer records, but by and large judges have been very accepting of computer records. The key to ascertaining the reliability of computer evidence is to assess the controls that make it reliable. This observation should come as no surprise to auditors, for they know they cannot rely on the information in a system unless the system is adequately controlled. Hence, the practical solution to the legal evidence concern is the same solution that applies to audit concerns: EDI systems need to be adequately controlled to ensure that the records the systems create are accurate. See Chapter 5 for a discussion on controls enhancing the EDI record credibility.

EDI raises a new control issue. In case of a disagreement between trading partners, what prevents one party or the other from forging or altering its records? A variety of controls might be instituted to address this problem. Some (such as cryptographic authentication) are more difficult and expensive to implement than others. The choice of controls for any particular implementation depends on many factors. See Chapters 4 and 5.

To best understand the nature of this choice, one should first consider the flaws of the medium EDI is replacing — paper. Commercial contracts written on paper are often several pages in length, but seldom are the pages held together with much more than a staple. What prevents the holder of a contract from lifting the staple and switching out a couple of pages? The physical properties of the paper provide weak safeguards against page switching.

One might argue that if one party switched out pages, a court could detect it. The new pages might have a different typestyle or a different quality of paper. But these special "forensic" qualities of paper were easily defeated. The careful wrongdoer would use the same typestyle and paper quality. Alternatively, the wrongdoer might say,

The reason pages 2 and 3 have typestyles and paper quality that are different from pages 1 and 4 is that the original party sent them to me in that condition. The original party deliberately wanted to create doubt in our minds today about the authenticity of pages 2 and 3. So, I tell you truthfully, this is the entire, authentic document!

So when we recognize paper’s shortcomings we realize fraud has historically not been prevented so much by the forensic properties of the medium of communication as by the wealth of facts and circumstances surrounding a business deal. One of the things that makes it difficult to change a document is the possi-
bility that the other party kept a copy. In addition, the other party may remember what the terms of the original document were. Thus, the document alterer may be buying herself nothing more than a nasty argument in court. And, if the wrongdoer is caught, she can be sued for fraud, and her reputation as a reputable business person will be tarnished.

Granted, it does require some effort and care to change a paper document. But, it also requires something to change an electronic document, namely: (1) access to the document, (2) the necessary software, (3) detailed knowledge of the deal between the parties, and (4) the recording of the document on an erasable medium. EDI systems can be designed to deny some or all of these to potential wrongdoers.

One idea is that a third party network would store copies of EDI messages as legal records. This proposal has hazards, however. The records, which are themselves valuable assets, would then be outside the immediate control of the user. Under the federal Electronic Communications Privacy Act of 1986, a government law enforcement agency can gain access to those records under some circumstances. What is more, the government can (sometimes) even force the third party network to delay for some period (such as 90 days) telling the user that the government is snooping through the user’s records. Users therefore prefer to keep their records under their own roof.

For most EDI implementations, the wiser approach is to design internal recordkeeping programs that simply deny items [1] through [4] above to the people who have an incentive to commit fraud. EDI systems can be designed, for example, so that transactions are automatically written to a non-erasable optical disk. Alternatively, trusted recordkeepers can be designated within user companies. These recordkeepers can store on magnetic tape (or other media) records of all EDI transmissions. The recordkeepers can be groups of employees who are insulated from the incentive to read and alter records. They can be denied the software and training necessary to make intelligent alterations of messages. These trusted recordkeepers would be similar to an independent “third party,” even though the user companies employ them. Chapters 4 and 5 discuss other controls that can contribute to making EDI records credible.

Many larger companies have formal record retention policies for all their records. Smaller companies should have such policies but often do not. These specify which records should be kept, the cataloguing systems that apply to the records and the dates records should be destroyed. Development of these policies takes into account many factors, such as retention costs, legal agreements, regulatory requirements, tax and audit needs and even antitrust concerns. The cost and antitrust factors militate toward destroying documents early. The others militate toward longer retention.

EDI implementors are well advised to reconcile their data retention practices with the overall corporate record retention policy. In larger corporations, this would involve contacting the corporate records retention manager (or committee). The corporate policy for paper documents will probably have specific retention periods for such documents as purchase orders, bills of lading and invoices. The EDI implementor needs to consider how these should apply to corresponding EDI transactions.

One problem is that EDI data may normally be retained in a chronological log, which mixes purchase orders, invoices and bills of lading. But the old record retention policy may call for each of those documents to be destroyed at a different time. The selective destruction of particular EDI transactions may not be practical without special planning.
Another issue is that EDI records need to be retained in a fashion that permits them to be read years later. It may be necessary, therefore, to keep EDI system documentation and software so that a future researcher can read records. This requires some foresight on the EDI implementor's part.

One particular recordkeeping law to bear in mind is tax law. Authorities expect taxpayers to keep records of transactions such as invoices and payments so the taxpayer declarations on tax returns can be substantiated. Traditionally, this meant that taxpayers kept original, paper-written invoices, checks and check stubs.

EDI's elimination of paper raises an issue. Taxpayers can keep computer records of transactions, but what assurance does the tax auditor have that they should be believed. For all the auditor knows, the taxpayer forged or changed them.

The United States Internal Revenue Service (IRS) has long maintained policies on the way in which corporate taxpayers must keep records of tax-related information that happens to be in computer format. These policies, embodied in Revenue Ruling 71-20 and Revenue Procedure 86-19, contemplate taxpayers keeping electronic records of accounting information (such as ledgers and journals), but they also contemplate those taxpayers keeping the original paper documents (such as invoices) that supported the information on the electronic records. As they stood prior to 1991, Rev. Rul. 71-20 and Rev. Proc. 86-19 were ambiguous and confusing in their application to EDI.

In October 1991, the IRS revised Rev. Proc. 86-19 by issuing Rev. Proc. 91-59 (see appendix to this chapter). Rev. Proc. 91-59 generally provided the following for corporate taxpayers having assets of at least $10 million:

1. The taxpayer need not make hardcopy (paper) records if they would not normally be created.
2. The taxpayer must keep electronic records of EDI transactions that have a tax relevance. These records, when combined with any other records the taxpayer keeps, must contain all the information required to be retained under the Internal Revenue Code for the relevant transactions.
3. The taxpayer need not institute any particular regime of controls over EDI records, but the taxpayer must retain documentation that describes the controls that are in place. Further, the taxpayer must be able to establish the “integrity” of its EDI records, and must reconcile its EDI records with its other books and records.

In effect, the IRS is saying that the taxpayer has considerable discretion. The taxpayer can keep some or all records on computer media, but the aggregate of its electronic and paper records must contain all the tax information relevant to the transactions conducted via EDI.

Further, the taxpayer must devise its own control methods and be prepared to show the Service that the methods chosen are adequate to make the records reliable. Ultimately, it is appropriate that the taxpayer bear the burden of establishing that its records are reliable. Still, it may be useful for the government to provide the taxpayer more guidance on what controls are necessary to satisfy government auditors.13

The IRS staff can assist the taxpayer in designing a particular recordkeeping program. Upon request, the local IRS District Director will assign an IRS EDP specialist to advise a taxpayer in a “record retention review.” The specialist is not likely to conduct a full analysis of the taxpayer's recordkeeping system or to give the taxpayer extensive advice. But with the District Director's approval the specialist may concur with specific suggestions from the taxpayer that certain records be destroyed. The initiative for identifying and suggesting which records to destroy probably must come from the taxpayer.
As of late 1994 state tax authorities were beginning to consider whether they should adopt recordkeeping regulations to cover EDI. The California Board of Equalization was circulating a draft amendment to its Sales and Use Tax Regulation 1698. The amendment adopts an approach that is similar to Rev. Proc. 91-59, with some variation.

**Vendor Agreements**

Unlike trading partner agreements, no models have been drafted for third party network agreements or EDI software agreements. Virtually all vendors of services and software, however, have their own "standard form" agreements that they ask customers to sign. These agreements are written by the vendors' counsel for the purposes of maximizing the vendors' rights and minimizing the vendors' exposure to liability.14

Customers are well advised to have counsel review these agreements before signing them. Vendors will often negotiate the terms of these agreements — up to a point.

A guiding principle for any customer negotiating a vendor agreement is that all important terms should be clearly written into the agreement. If a customer expects the vendor to satisfy a particular technical requirement or provide a service promised in a sales pitch, the customer wants the contract to reflect that requirement or service. The typical vendor contract contains an "integration" clause stating that the contract embodies the entire and exclusive agreement between the parties. So if the agreement does not contain a term the customer had bargained for, it is doubtful the customer can enforce that term.

Another general principle to observe with vendor agreements is that technical words need to be defined carefully. Information technology terms mean different things to different people. The more thorough the definition of terms, the less room there is for misunderstanding.

Most vendor agreements contain clauses limiting (1) the warranties for the service or product provided and (2) the vendor's liability under the agreement. The first clause might say that the vendor does not warrant that the service or software is fit for the customer's particular purpose. This clause might come as a rude surprise to a customer who has specifically described to the vendor the purposes the customer expects the service or software to achieve! In effect, this type of clause reduces the number of grounds on which the vendor might ever be in breach of the contract.

The second clause might say that if the vendor breaches the contract, the vendor's liability will not exceed some portion of the fees or price paid by the customer. It is likely to exclude any vendor liability for consequential damages, such as the profits the customer would lose if the vendor's product failed. The vendor's argument in favor of this clause is that the vendor should not accept significant liability for its errors because the customer is in a better position to protect against losses.15 Irrespective of that argument's validity, it points out that the wise customer will consider what backup systems and other controls are in place to protect it from shortcomings in the vendor's performance.

A customer desires that its data remain confidential. It may also wish to restrict the freedom of a third party network to monitor the volume and direction of customer data traffic and to build statistical analyses of that traffic. Such information could be competitively very sensitive. A customer can insist that appropriate clauses to protect the customer be stitched into the third party network agreement.
Sometimes EDI system auditors need assurance that third party network systems function properly and are adequately controlled. Auditors may obtain that assurance by auditing the systems directly or by receiving reports from other auditors who have audited the systems. Such reports are called "third party reviews." To prepare for any potential auditor requests, a customer could add to the third party network agreement clauses requiring the third party to maintain appropriate control and system documentation, and to periodically provide the customer's auditors either an appropriate third party review or access to the systems, documentation and network staff necessary to conduct an audit.

Software Agreements

A software developer seldom "sells" software to its customer. It "licenses" the software's use. The license usually restricts use to a particular customer site or to a stated number of customer computers. Use beyond that authorized in the agreement causes the customer to breach the agreement. Software developers' agreements often contain clauses that designate the developer as the only party authorized to update or maintain the software. (EDI translation software must regularly be updated because EDI standards regularly change.) This provision is not in the customer's interest. The customer prefers the flexibility to hire others to maintain the software in case the customer and the developer have a falling out. The customer also prefers that the maintenance clause limit the amount by which the developer may increase its maintenance fee each year.

Special Regulations

Companies operating in particular industries, or particular countries, may be subject to unique regulatory requirements that affect EDI implementation. The regulations may mandate that special language appear on a purchase order or an invoice, or may set specific recordkeeping and control requirements for company transactions. Depending on the situation, the regulations may either explicitly or implicitly demand paper writing. When EDI implementors encounter such regulations, the laws may need to be changed or the government may need to waive or reinterpret the requirements.

For example, some Department of Transportation regulations pertaining to the communication of hazardous materials information between a cargo shipper and a railroad carrier might be construed to require the exchange of paper-written information. The Department, however, has issued special waivers to some railroads permitting specified hazardous materials information to be communicated via EDI under certain conditions.

Sometimes, however, government agencies will be reluctant to interpret ambiguous laws to allow electronic communication. Texas sales tax regulations, for example, provide an exemption from tax on a sale if the buyer gives the seller an appropriate certificate. The Texas Comptroller of Public Accounts prescribes the form of the certificate, and that form today requires a signature. The relevant statute, adopted by the state legislature, requires that the certificate be "written." One Texas EDI user requested that the Comptroller rule that an electronically transmitted certificate can be deemed "signed" and "written." The Comptroller's office did not believe it had the power to issue such a ruling. Moreover, the Comptroller's office felt its auditors would not be equipped to detect fraud in electronic certificates as well as they could in paper certificates.

Problems such as that in Texas necessitate better education of government authorities, and in some cases, appeal to legislatures to amend the law.
EDI presents legal and audit professionals some novel challenges. The application of laws, rules and principles to EDI transactions may sometimes be unclear. Lawyers and auditors may be unable to use traditional devices (such as ink autographs) to accomplish evidence, control and other goals. EDI thus demands innovative thinking and the exercise of judgment. It also demands reeducation.

Eventually, all legal issues in EDI can be addressed. Paper and ink are just one among many means for recording and controlling information. Electronic methods can replace them. Lawyers and auditors should not shrink from these challenges. Their clients rightfully expect insightful analysis and creative solutions, not roadblocks. Ultimately, many of these challenges boil down to an assessment of risk and reward. Seldom do the risks involve criminal or moral matters. Instead, they usually involve merely economic risks, something businesses deal with day in and day out.

EDI is an immensely valuable technology. It promotes efficiency and productivity. Companies implementing EDI can reap tremendous cost savings, respond more quickly to changes in the market and realize critical strategic objectives. Often, the rewards of using EDI far outweigh any of the legal risks involved. Creative thinking can minimize those legal risks considerably.

The sale of goods, and related activities such as their transport, insurance and financing, is invariably accompanied by a movement of information. For the past several hundred years paper-based documents, in the form of contracts, purchase orders, invoices, bills of lading, and so on, have served as the predominant means by which to record this and other forms of commercial information. Over the past twenty years, however, developments in the areas of computers and telecommunications have created technologies that allow such paper-based documents to be replaced by direct computer-to-computer communications using a public or industry standard format. This latter practice, generally known as electronic data interchange (EDI), promises huge benefits to businesses and other organizations involved in commerce given that through EDI more accurate and more timely information can be exchanged for less cost than is the case with paper-based documents. Such a compelling combination of advantages likely will ensure the continued rapid growth of EDI in an ever increasing number of commercial and administrative settings.

The substitution of EDI for paper-based documents presents numerous technical, control and legal challenges. EDI raises numerous legal questions because in so many respects it differs from the paper-based mode of collecting, storing, presenting and transmitting information. Paper-based documents are durable and can remain in existence for many years. Alterations to paper documents can be detected quite readily. Documents on paper can be conveniently authenticated by personal signatures or by other means. Most importantly, legal systems around the world have had some two hundred years, and in some cases even longer, to develop a comprehensive system of statutory and judge-made rules governing all aspects of the use of paper-based documents in commerce. Familiarity, among other things, breeds reliable legal precedent. Today business people and their legal advisors have a very good idea of how the law will treat a

---

† Section II was written by George S. Takach, Partner, McCarthy Tétrault, Toronto. © Copyright George S. Takach 1995.
particular question relating to a paper-based document, such as whether a certain document is admissible in a legal proceeding, because either a specific provision in a statute addresses, or a previous decision of a judge has addressed, the question.

The same cannot be said with respect to EDI. While there exist various technical means to help ensure the "durability," "non-alterability" and "authenticity" of information that is collected, stored, presented and transmitted electronically, legal systems have yet to amend statutory rules sufficiently, or produce judicial decisions, in order that EDI be accorded the same legal certainty as paper-based documents. Many, many questions remain unanswered. These questions, and the uncertainty caused by them, in most cases will not present an insurmountable hurdle to the implementation of EDI in any particular setting. Managers responsible for EDI, however, should be sensitive to these questions, should come to understand them with the assistance of legal counsel, and then should plan to implement EDI in a manner that reduces, as much as possible, the uncertainty caused by them.

Contract Law

Issues

Several rules of contract law strive to ensure that parties to a contract create a reliable record of their contractual commitments so that, if there is any dispute between the parties as to their respective contractual obligations, it is clear what the parties agreed to in their contract. Thus in Canada, and in many other jurisdictions, certain contracts must be made in "writing" and must be "signed" by the parties to the contract. Rules have also been developed regarding the formation of contracts, such as the rules regarding "delivery" of written documents intended to create contractual obligations so as to determine when and where a contract has come into existence. Numerous rules also exist to govern the rights and obligations flowing from certain documents used in international trade. In each of these areas EDI poses a challenge to the traditional legal rules.

Legislation exists in many jurisdictions requiring that certain contracts be in "writing." For example, the legislation in several Canadian provinces that govern the sale of goods provides that contracts for the future delivery of goods are not enforceable unless they are "in writing." Moreover, in these jurisdictions it is often not clear whether a "writing" can include anything that is not visible to the unaided eye. As a result, the important question arises whether, under these rules of law, EDI may be used to create enforceable contracts.

There will not be a definitive answer to this question until the courts answer it, or until laws are passed that expressly recognize EDI messages as being capable of creating legally binding commitments. Until one of these solutions comes to pass, the best that businesses and other organizations using EDI can do is to address the "writing issue" in their EDI trading partner agreements (TPAs). Fortunately, in December 1994 the Province of Ontario, Canada’s most important province commercially speaking, amended its Sale of Goods Act to delete the writing requirement, thereby benefitting users of EDI in that province.

Many of the same statutes that require certain agreements to be in writing also stipulate that they be "signed" by the parties to the agreement. The "signature issue," however, is less problematic in Canada than the "writing issue" because rather than being defined generally in a statute, the term "signature" may be interpreted with flexibility by judges. Indeed in a recent case the answer back of the sender of a telex was mentioned as constituting a signature. Nevertheless, it is still sensible to address the signature issue in a TPA.
EDI also raises some contract formation questions. In order to form a contract there must be, among other things, an offer from one party and an acceptance of that offer by another party. In situations where there is simultaneous conveyance of offer and acceptance in one place, such as in face-to-face negotiations and contract signings, there is rarely an issue regarding when and where the contract was made. Where there are not simultaneous negotiations and communication in one place, the general rule has developed in Anglo-Canadian jurisprudence that an offer is not accepted until the acceptance of the offer is communicated to the offeror. Some 100 years ago in the U.K. an exception to this rule was developed by judges for offers and acceptances sent by mail. The so-called "post box" rule holds that where an offer is made by the mail, the contract is made immediately at the time the acceptance is posted in the mail (rather than when the acceptance is actually received by the offeror) where use of the mail is reasonable in the circumstances or expressly contemplated by the parties.

It may be asked whether this "post box" doctrine would apply to EDI. It might in the case where an EDI message is sent not directly to the intended EDI trading partner, but rather to a third party EDI service provider (a VAN) who holds the message for some period until the intended recipient retrieves it electronically from the service provider. By contrast, the "post box" doctrine likely would not apply to EDI messages that are transmitted directly between trading partners, given that such a relationship approximates more closely instantaneous communication of offer and acceptance. In this regard it is interesting to note that the courts have not applied the "post box" doctrine to telex communications, but rather for such means of "nearly instantaneous" communication the courts will look at a variety of factors to determine when a contract came into existence. Given that this judicial rule for telex communications leaves each court with a fair degree of discretion, and assuming a similar approach would be taken to EDI, again it is recommended that trading partners deal with the contract formation issues of when and where a contractual commitment first arose in their TPA.

In addition to the question "when does a contract concluded by EDI arise?," it will often be relevant to ask "where" such a contract arises. This is an important question because it determines, among other things, which jurisdiction's laws would govern the parties' EDI relations. This question might never have to be asked if all the relevant parties are located in the same jurisdiction, such as a single province in Canada. By contrast, consider the following situation. One EDI trading partner is located in France and the other is in Ontario, and they communicate through the French trading partner's network provider, who is located in England and the Ontario trading partner's network provider, who is located in Ohio. If there is a problem with an EDI transmission that causes damages to one or more of these parties, which of French, Ontario, English or Ohio law should be applied to the claim? Rather than having to rely on general, and often difficult to apply, legal principles to answer such a question, it is preferable for EDI trading partners to stipulate in their TPAs, and in their agreements with network providers, which jurisdiction's law will govern any possible claims.

It should be noted that while to-date (February 1995) there have been no reported court cases in Canada that have dealt with the contract law issues raised by EDI, in a couple of cases courts have decided that faxes of signed documents satisfy certain "signed writing" requirements. In these cases judges have noted that the law has tried to be receptive to "technological advances in the means of communications." These same judges, however, also recognize that each technology must be assessed on its own merits, and they understood that the fax technology before them essentially involved making a copy of a signed original, albeit by a
fax machine. EDI, however, does not resemble this photocopying technology in many important aspects, so it remains to be seen how the principles in these cases will be applied to EDI.

One further development is worth noting in respect of the writing issue. In May 1992 the Canadian provinces adopted the United Nations Convention On Contracts for the International Sale of Goods.20 Under this convention, contracts for the sale of goods between persons in different countries need not be in writing. Accordingly, if a company in Canada wants to sell goods to a company in the U.S., and these companies want to use EDI to create specific sales contracts, they could invoke the Convention in order to override, in effect, the writing requirement in any applicable provincial or state legislation.

In the same vein, it is important to review if the particular jurisdiction in which an EDI trading partner is located has a writing requirement in its goods legislation. For example, neither Ontario nor British Columbia have such a writing requirement in their respective sale of goods legislation, and therefore a company in a province with a writing requirement conducting EDI with an Ontario or B.C. company should provide that Ontario or B.C. will be the governing law of their EDI trading partner agreement.

Evidence Law

Issues

The rules of evidence law strive to ensure that only reliable evidence is admitted and relied upon in court and other legal proceedings. With respect to common law jurisdictions, there are two rules of evidence law that are often considered to pose a challenge to the admissibility as evidence of computer-generated records, which would include EDI messages. The first is the "hearsay rule," which stipulates that, whenever possible, evidence should be obtained orally from witnesses as this form of evidence can be subject to cross-examination and other forms of truth testing. In the context of written evidence the hearsay rule, if strictly applied, would require that a document is not admissible unless its author is present in court to attest to its contents. The second rule of evidence is the so-called "best evidence rule," whereby a document is admissible only if it is produced in its original version.

In recognition, however, of the increasing reliability of record keeping in modern businesses, statutes governing the law of evidence have been passed in most of Canada provinces that allow certain types of "business records" to be admissible as evidence under certain conditions. These statutory rules, however, were not drafted with EDI in mind, and hence it may be asked whether copies of EDI messages would be admissible in court and other legal proceedings. No court has yet had occasion to determine whether an EDI message should be admissible under such a statute. Courts in Canada have considered, however, whether computer generated records are admissible under these rules, and generally they have been admitted so long as the computer and the related record taking and record keeping procedures can be shown to be trustworthy.21

Accordingly, EDI trading partners should do at least two things to help ensure that their EDI messages are held to be admissible in court or other legal proceedings. First, they should address the issue in their TPA. Second, they should institute appropriate computer security, control and other measures to ensure that their EDI message making and recording systems are as trustworthy as possible. This would entail, for example, storing EDI messages on non-alterable media that permit only read and copy, but not write, access.
Record Retention Issues

A similar issue to the evidence law one arises in connection with the record retention requirements stipulated by numerous statutes in many jurisdictions. For example, Canada's Income Tax Act requires businesses to keep certain books of account and records which, among other things, permit the taxes payable or the taxes or other amounts to be collected by a person, to be determined. It is interesting to note that the government department in Canada that administers this tax statute (Revenue Canada) permits companies to keep microfilm copies of books and records of original entry and source documents, provided the microfilming process utilized complies with a certain standard produced by the Canadian General Standards Board and approved by the Standards Council of Canada.22

With the recent updating of this standard to cover electronic imaging procedures, Revenue Canada has indicated orally that it will accept for records retention purposes images that are made pursuant to the updated standard. It is expected that formal recognition of this new policy will be forthcoming with an appropriate amendment to Revenue Canada's written policy on records retention. As for EDI, it would appear that Revenue Canada takes the view that EDI messages should be acceptable for records retention purposes under Canada's income tax law as being original "source documents," and thus Revenue Canada has indicated that paper-based copies of EDI messages need not be created or retained for records retention purposes. It would be useful, however, if this position regarding EDI were clearly confirmed in Revenue Canada's written policy on records retention. In any event, users of EDI may wish to approach Revenue Canada or other relevant government departments to discuss their particular circumstances so that they are able to establish electronic recording keeping measures that will satisfy the applicable public authorities.

Trading Partner Agreements

Based on the discussion above, it should be clear that all EDI trading partners should enter into TPAs before commencing to do business with one another through EDI. Unfortunately, it is probably the case that a great deal of EDI activity is not underpinned by TPAs. This is a mistake. Particularly as the use of EDI increases, such that organizations increasingly use EDI not only for their biggest and best customers (but also for smaller and less established customers), it becomes imperative that EDI trading partners implement TPAs.

The TPA should deal with the technical aspects of the relationship, such as the precise EDI protocol to be utilized, together with the particular verification, authentication and security procedures to be employed. As noted above, the "writing," "signature," and other contract law and "evidence law" issues should also be addressed in the TPA. For example, the parties should acknowledge in the TPA that properly recorded and authenticated EDI messages are to be considered to be signed writings, and that neither party will contest their admissibility as evidence. It is also a good idea for the EDI trading partners to agree to a process in the TPA whereby contractually binding commitments will arise only if certain predetermined EDI messages, including an acceptance message, are exchanged.

The EDI trading partners should also decide what terms and conditions will govern the underlying transaction effected by EDI. For example, the provisions
relating to product warranties, limitations of liability, and so on. In a non-EDI environment these issues are often left up to the so-called “battle of the forms,” whereby each side hopes that the terms on its purchase order or other document will prevail in the event of a dispute. The EDI environment does not lend itself to fighting a battle of the forms through the transmission of EDI messages. Some parties, nevertheless, try to perpetuate this battle by attaching the contract documents of both parties to the TPA and stipulating that these various forms will apply as if they were actually used (but they are not, as the EDI messages are being sent instead). This results in a very uncertain, unsatisfactory state of affairs.

The preferred solution is for the EDI trading partners to negotiate a mutually acceptable set of terms and conditions that will apply to the underlying sales or other transactions. This may require an investment of some time and effort by business people and legal counsel, but it is an investment that will pay significant dividends, even if there is never a dispute between the parties.

It is worth noting that the EDI Council of Canada has published a model TPA, together with a commentary on the various provisions in it. This is an extremely useful document and it should probably serve as the starting point for the drafting of most TPAs between EDI trading partners. The model TPA, however, does not have all the answers. It contains, for example, numerous sections in square brackets which deserve particular scrutiny to determine whether they should be used by the trading partners. In short, the parties to an EDI relationship must always modify the model TPA to suit their particular circumstances.

It should also be noted that a TPA, however comprehensive it might be, will never be able to dispel completely the legal uncertainty that currently exists in respect of the “writing” and evidence law and records retention issues. The only really effective resolution of these issues will come when laws in Canada, and elsewhere, are amended to recognize expressly EDI and other forms of electronic commerce (such as document imaging systems). Accordingly, organizations utilizing EDI should support the law reform efforts of organizations like the EDI Council of Canada so that a more certain legal environment for EDI can be established as soon as possible. Until then, parties considering implementing EDI should review with their legal counsel the particular use to be made of EDI, the legal risks posed by such EDI usage, and the contractual and other methods available to reduce and effectively manage this risk.

Organizations that communicate to one another through EDI often do not do so directly. Rather, one or both parties may use the services of a third party network provider. A network provider will serve several functions, including collecting and forwarding EDI messages, as well as conducting message authentication, audit and other services. A particularly valuable service of a network provider is serving as an intermediary between two EDI trading partners with incompatible systems.

A network provider invariably makes available its services to a customer only after the customer has entered into a “network services” or similar agreement. This agreement will define the various services to be provided by the network provider, and it will set out the terms and conditions under which the services will be provided. A customer of a network provider will generally want to ensure that this agreement addresses a number of issues important to the customer.
One of these is confidentiality. The customer will want to be satisfied that the agreement requires the network provider take adequate measures to safeguard the confidentiality of the customer’s EDI messages. Another issue involves the availability of the services; the customer may want to provide in the contract that the network provider’s computer and telecommunications system will be unavailable no more than a specified (and few) number of hours each week or month if system availability is important to the customer (and it is to most users of EDI!). Similarly, the agreement might provide that failure to meet such performance guarantees will result in the customer accumulating financial credits against service fees otherwise payable, in addition to exercising any other remedies available to the customer.

With respect to this latter point, it is important to note that virtually all standard form network provider agreements will contain a provision limiting the liability of the network provider in the event it has caused the customer some damage. These sorts of clauses, as well as the warranty disclaimers invariably found in network provider agreements, should be carefully scrutinized to ensure that they are reasonable from the customer’s perspective. In effect, as with EDI trading partner agreements, agreements with network providers should be reviewed carefully with legal counsel to ensure that they address all issues relevant to the customer.
References


4. One example of a statute of frauds is Uniform Commercial Code Section 2-201, which provides:

   [A] contract for the sale of goods for the price of $500 or more is not enforceable unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker. A writing is not insufficient because it omits or incorrectly states a term agreed upon but the contract is not enforceable under this paragraph beyond the quantity of goods shown in such writing.

   The Uniform Commercial Code is a statute in force in whole or in part in all states in the United States. Article Two of the Uniform Commercial Code (of which Section 2-201 is a part) governs sales of goods transactions.


12. *The Law of Electronic Commerce*, for discussions of U.S. v. Poindexter, a high-profile criminal trial in which a record of an electronic mail message was admitted into evidence. One factor that appeared to contribute to the reliability of the record was that the record keeper was segregated from the message creator and the prosecutors who used the message in court.


17. Texas Tax Code Section 151.155.


20. In Ontario, for example, see the International Sale of Goods Act, R.S.O. 1990, Ch. I.10.


22. Revenue Canada’s policies on record retention are set out in information Circular No. 78-10R2, July 14, 1989. The original microfilm standard was; Microfilm as Documentary Evidence, Canadian General Standards Board (CAN 72.11-88). The new Microfilm and Electronic Images as Documentary Evidence Standard is CAN/CGSB-72.11-93 of the Canadian General Standards Board; this current standard supersedes CAN 72.11-88.
Chapter 7 Appendix A: Trading Partner Agreement Model

The following represents an outline model of the various clauses expected to be included in a typical TPA agreement. Generally, a TPA would cover these core clauses. It remains a matter of tailoring according to the specific local governing laws and adding whatever other clauses the contracting parties, assisted by legal counsel, would choose to include. This is the case for the American Bar Association (ABA) TPA model, the EDI Council of Canada TPA model, prepared by the Legal and Audit Committee, the Australian model and various European models.

Outline

1. Identification of EDI standards
2. Identification of third party service providers
3. Obligation to conduct EDI competently
4. Adoption of signatures
5. Place and time of message receipt
6. Functional acknowledgments
7. Application acknowledgments
8. Garbled transmissions
9. Trade terms and conditions
10. Disclaimer of confidentiality
11. Legal enforceability of transactions
12. Termination of agreement
13. Disclaimer of obligation to enter into transactions
14. Limitation of liability
15. Arbitration

The American Bar Association Model EDI Trading Partner Agreement can be purchased from the ABA by calling (312) 988-5555 and requesting document number: 507-0233-B9. Or simply write to:

- American Bar Association
  Order Fulfillment Department
  750 North Lake Shore Drive
  Chicago, IL 60611

For the Canadian Model, you may contact the EDI Council of Canada. The document is called, *Electronic Data Interchange Trading Partner Agreement and Commentary*. This document contains explanations of the various clauses with appropriate expert commentaries from the committee. Phone: (416) 621-7160, FAX: (416) 620-9175. Or write to:

- EDI Council of Canada
  5401 Eglinton West, Suite 203
  Etobicoke, Ontario
  M9C 5K6
EDI CONTROL, MANAGEMENT, AND AUDIT ISSUES

The European Commission, Model Trading Partner Agreement, contact:

■ European Commission
  Rue de la Loi 200
  B-1049 Brussels, Belgium

For International Interchange, the Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission (UNCID).

■ International Chamber of Commerce
  ICC Publishing Corporation
  156 Fifth Avenue
  New York, NY 10010
26 CFR 601.105: Examination of returns and claims for refund, credits or abatement; determination of correct tax liability. (Also Part I. Section 6001; 1.6001-1.)

Rev. Proc. 91-59

SEC. 1. PURPOSE

.01 The purpose of this revenue procedure is to update Rev. Proc. 86-19, 1986-1 C.B. 558, and to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer's records are maintained within an Automatic Data Processing (ADP) system. Rev. Proc. 86-19 provides guidelines for record requirements to be followed in cases where all or part of the accounting records are maintained within an ADP system. References to ADP systems include all accounting and/or financial systems and subsystems that process all or part of a taxpayer's transactions, records, or data by other than manual methods.

.02 The technology of ADP has evolved rapidly, and new methods and techniques are constantly being devised and adopted. The requirements set forth in Section 5 of this revenue procedure are intended to ensure that all machine-sensible records generated by a taxpayer's ADP system are retained so long as they may be or may become material in the administration of any internal revenue law. These requirements will be modified and amended as needed to keep pace with developments in ADP systems.

SEC. 2. BACKGROUND

.01 Section 6001 of the Internal Revenue Code provides that every person liable for any tax imposed by the Code, or for the collection thereof, shall keep the records that the Secretary may from time to time prescribe.

.02 Rev. Rul. 71-20, 1971-1 C.B. 392, establishes that all machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer's ADP system are records within the meaning of section 6001 of the Code and section 1.6001-1 of the Income Tax Regulations, and are required to be retained so long as the contents may be material in the administration of any internal revenue law.

SEC. 3. SCOPE

.01 This revenue procedure encompasses all types of data processing systems including, but not limited to, microcomputer systems, Data Base Management Systems (DBMS), and all systems using Electronic Data Interchange (EDI) technology. For purposes of this revenue procedure: DBMS means a software system that creates, controls, retrieves, and provides accessibility to data stored in a database; and EDI technology means the computer-to-computer exchange of business information.

.02 The utilization of a service bureau, time-sharing service, or value-added network does not relieve the taxpayer of the responsibilities described in this revenue procedure.

.03 A taxpayer with assets of $10 million or more at the end of its taxable year shall comply with the record retention requirements of Rev. Rul. 71-20 and the provisions of this revenue procedure. For purposes of this revenue procedure, a controlled group of corporations, as defined in section 1563 of the Code, will be considered to be one corporation and all assets of all members of the group will be aggregated.

.04 A taxpayer with assets of less than $10 million shall comply with the record retention requirements of Rev. Rul. 71-20 and the provisions of this revenue procedure if any of the following conditions exist:

1. information required by section 6001 of the Code is not in the hardcopy books and records, but is available in machine-sensible records;

2. machine-sensible records were used for computations that cannot be reasonably verified or recomputed without using a computer (e.g., Last-In, First-Out (LIFO) inventories); or

3. the taxpayer is notified by the District Director that machine-sensible records must be retained to meet the requirements of section 6001 of the Code.

.05 The requirements of this revenue procedure pertain to all matters under the jurisdiction of the Commissioner of Internal Revenue including, but not limited to, income, excise, employment, and estate and gift taxes, as well as employee plans and exempt organizations.

.06 The requirements of this revenue procedure are applicable to the machine-sensible records generated by a Controlled Foreign Corporation (CFC), a domestic corporation that is 25 percent foreign-owned, and foreign corporations engaged in a trade or business within the United States at any time during a taxable year because the definition of "records" in sections 964(c), 982(d), 6038A and 6038C of the Code and the regulations thereunder has the same meaning as "records" as used in section 6001 of the Code and section 1.6001-1(a) of the regulations.

.07 Machine-sensible records used by an insurance company to determine losses incurred under section 832(b)(5) of the Code shall be retained in accordance with the requirements of this revenue procedure and Rev. Proc. 75-56 1975-2 C.B. 596. For this purpose, the machine-sensible files for a particular taxable year include the files for that year and the seven preceding years, all of which shall be retained so long as they are material to the examination of the federal tax return. See section 5.06 for a discussion of materiality.

.08 The requirements of this revenue procedure are
applicable to any sections of the Code that have unique or specific recordkeeping requirements. For example, machine-sensible records maintained by the taxpayer to meet the requirements of section 274(d) relating to the amount, time, and place of a business expense must meet the requirements of this revenue procedure.

SEC. 4. DISTRICT DIRECTOR AUTHORITY

.01 In the case of a taxpayer that has less than $10 million in assets at the end of its taxable year, the District Director may notify a taxpayer that machine-sensible records must be retained to meet the requirements of section 6001 of the Code, and that Rev. Rul. 71-20 and the provisions of this revenue procedure apply to that taxpayer. Subsequent failure to comply with this notification may result in the imposition of the penalties described in section 7.

.02 The District Director has the authority to enter into or revoke a record retention limitation agreement with the taxpayer to modify or waive all or any of the specific requirements in this revenue procedure. The taxpayer remains subject to all requirements of this revenue procedure that are not specifically modified or waived by a record retention limitation agreement. A taxpayer that has questions regarding the application of this revenue procedure to a specific factual situation should contact the appropriate District Director.

(1) A record retention limitation agreement does not apply to a subsidiary company acquired, or accounting and tax systems added, subsequent to the completion of the record evaluation (see section 3.03 below) upon which the agreement is based. All machine-sensible records produced by a subsequently acquired company or a subsequently added accounting and tax system whose contents may be or may become material in the administration of the Code shall be retained by the taxpayer who signed the agreement until a new evaluation is conducted by the District Director.

(2) Upon the disposition of a subsidiary, the files being retained for the Service by, or for, the disposed subsidiary shall be retained by the taxpayer until a new evaluation can be made by the District Director.

.03 To determine if a taxpayer may limit its retention of machine-sensible records, a record evaluation may be conducted by the District Director. This evaluation of the data processing and accounting systems may be initiated by the District Director or requested by the taxpayer, and is not an “examination,” “investigation,” or “inspection” of the books and records within the meaning of section 7605(b) of the Code because these tests are not directly related to the determination of tax liability for a particular taxable period.

.04 The District Director may periodically initiate tests to establish the authenticity, readability, completeness, and integrity of the machine-sensible records retained as required by this revenue procedure. These tests may include the testing of EDI and/or other procedures, and a review of the internal controls and security procedures associated with the creation and storage of the records. These tests are not an “examination,” “investigation,” or “inspection” of the books and records within the meaning of section 7605(b) of the Code because these tests are not directly related to the determination of tax liability for a particular taxable period.

SEC. 5. MACHINE-SENSIBLE RECORDKEEPING REQUIREMENTS

.01 All machine-sensible records whose contents may be or may become material to the administration of the Code shall be retained by the taxpayer. The retained records shall be in a retrievable format that provides the information necessary to determine the correct tax liability. The taxpayer shall ensure that the details and the source documents underlying any summary accounting data may be easily identified and made available to the Service upon request.

.02 Documentation that provides a complete description of the ADP portion of the accounting system, including all subsystems and files that feed into the accounting system, shall be retained and made available to the Service upon request. The statements and illustrations as to the scope of operations shall be sufficiently detailed to indicate:

(1) the application being performed;
(2) the procedures employed in each application;
(3) the controls used to ensure accurate and reliable processing; and
(4) the controls used to prevent the unauthorized addition, alteration, or deletion of retained records.

.03 The following specific documentation for all retained files shall also be kept:

(1) record formats (including the meaning of all “codes” used to represent information);
(2) flowcharts for a system and a program;
(3) label descriptions;
(4) source program listings of programs that created the retained files;
(5) detailed charts of accounts (for specific periods);
(6) evidence that periodic checks of the retained records that are prescribed in section 5.08 were performed; and
(7) evidence that the retained records reconcile to the books and the tax return. This reconciliation shall establish the relationship between the total of the amounts in the retained records by account to the account totals in the books and to the tax return.

.04 Any change to the ADP system which affects the accounting system and/or subsystems, together with their effective dates, shall be documented in order to preserve an accurate chronological record. This documentation shall include any changes to software or systems and any changes to the formats of files.

.05 In addition to the documentation described in section 5.02 Through 5.04, the service may require that the taxpayer furnish any other evidence (e.g., internal audit reports) that pertains to the authenticity and integrity of the records.
.06 Machine-sensible records are required to be retained until their contents are no longer material to the administration of the Code. At a minimum, this materiality continues until the expiration of the statute of limitations, including extensions, for each tax year. In certain situations, records should be kept for a longer period of time. For example, records that pertain to fixed assets, losses incurred under section 832(b)(5) of the Code, and LIFO inventories should be kept for longer periods of time.

.07 All machine-sensible records that must be retained shall be clearly labelled and stored in a secure environment. For example, supplemental labels with the statement “Tax Year 19XX Records — Retain for IRS until 0000” or “Retain for IRS, Consult Tax Manager Before Releasing” should be used and affixed to each tape reel, cartridge, disk pack, diskette, or other device being retained, and a retention date should be written on the internal label. Back-up copies of machine-sensible records retained for the Service should be stored at an off-site location. The Service recommends that taxpayers refer to the National Archives and Record Administration’s (NARA) standards for additional guidance on the maintenance and storage of electronic records. See, Standards for the Creation, Use, Preservation, and Disposition of Electronic Records, 36 C.F.R. Ch. XII, Part 1294, Subpart C(1990).

.08 The taxpayer shall make periodic checks on all records retained for the Service. The Service recommends using the NARA standard for making periodic checks of retained machine-sensible records. See, 36 C.F.R. §1254.28(g) (4)(1990). In general, this standard requires a recordkeeper to annually select and test a random sample of all reels of magnetic tape to identify any loss of data, and to discover and correct the causes of data loss. In libraries with 1800 or fewer storage units (e.g., magnetic tape reels), a 20 percent random sample or a sample size of 50 units, whichever is larger, shall be read. In libraries with more than 1800 units, a sample of 384 units shall be read.

.09 If any machine-sensible records required to be retained are lost, destroyed, damaged, or found to be incomplete or materially inaccurate, the taxpayer shall report this to the District Director and recreate the files within a reasonable period of time.

.10 Although the NARA sampling standard referred to in section 5.09 is specifically for magnetic computer tape, the Service recommends that all retained machine-sensible media be randomly sampled and tested as described by NARA. A taxpayer whose data maintenance practices conform with the NARA standards and who loses only a portion of the data from a particular storage unit will not be subject to the penalties described in section 7. However, this taxpayer remains responsible for substantiating the information on its return as required by section 6001 of the Code.

.11 The taxpayer must be able to process the retained records at the time of a Service examination. Processing shall include the ability to print a hardcopy of any record. When the data processing system that created the records is being replaced by a system with which the records would be incompatible, the taxpayer shall convert pre-existing records to a format that is compatible with the new system. Any changes in the ability to process the retained records shall be reported to the District Director.

.12 The taxpayer shall provide the Service, at the time of an examination, with computer resources (e.g., terminal access, computer time, personnel, etc.) that are necessary for the processing of the retained records. Failure to provide these resources will be a failure to maintain books and records under section 6001 of the Code.

.13 The use of a DBMS necessitates the implementation of procedures to ensure that appropriate records and documentation are retained. A taxpayer is in compliance with the provisions of this revenue procedure if a sequential file exists and is available to the Service. The sequential file shall contain the detail necessary to identify the underlying source documents. The process to create a sequential file should be reviewed by the District Director prior to destruction of the DBMS records. Sections 5.01 through 5.12 of this procedure shall apply to the resultant sequential file(s).

.14 In addition to the documentation described in section 5.02 through 5.05, the following documentation pertaining to each DBMS system shall be retained:

1. Data Base Description (DBD);
2. Record layout of each segment with respect to the fields in the segment;
3. Systems Control Language;
4. Program Specification Block (PSB); and
5. Program Communication Block (PCB).

.15 In order to be in compliance with this revenue procedure, a taxpayer that uses EDI technology must retain machine-sensible records that, in combination with any other records (e.g., the underlying contracts, price lists, and price changes), contain all of the detailed information required by section 6001 of the Code. The extent of the detail in the retained electronic and other records, if any, must be equivalent to the level of detail contained in an acceptable paper record. For example, the retained records for an electronic invoice must contain identification of the vendor by name, invoice date, product description, quantity purchased, price, etc. The taxpayer may capture this information at any level within the accounting system provided the audit trail, authenticity, and integrity of the retained records can be established.

SEC. 6. IMPACT ON HARDCOPY RECORDKEEPING REQUIREMENTS

01. Except as otherwise provided in this section, the provisions of this revenue procedure do not relieve taxpayers of the responsibility to retain hardcopy records that are created or received in the ordinary course of business as required by existing law and regulations.
Hardcopy records may be retained in microfiche or microfilm format in accordance with the requirements outlined in Rev. Proc. 81-46, 1981-2 C.B. 621. These records are not a substitute for the machine-sensible records required to be retained by this revenue procedure.

.02 Hardcopy records generated at the time of a transaction (e.g., credit card receipts) need not be retained if all the details relating to the transaction are subsequently received by the taxpayer in an EDI transaction and are retained by the taxpayer in accordance with this revenue procedure.

.03 If hardcopy records are not produced or received in the ordinary course of transacting business (as may be the case when utilizing EDI technology), or are not retained pursuant to section 6.02, hardcopy printouts of computerized records need not be created unless requested by the Service. These requests may be made either at the time of an examination or in conjunction with the testing described in section 4.04.

.04 Computer printouts that are created for validation, control, or other temporary purposes need not be retained.

SEC. 7. PENALTIES

The District Director may issue a Notice of Inadequate Records pursuant to section 1.6001-1(d) of the regulations if machine-sensible records are not properly retained as required by this revenue procedure. Failure to comply with the provisions of this revenue procedure may also result in the imposition of an accuracy related civil penalty under section 6662(a) of the Code that is attributable to negligence or disregard of rules or regulations as provided under section 6662(b)(1). A criminal penalty under section 7203 may also be applicable. See Rev. Rul. 81-205, 1981-2 C.B. 225, which explains the applicability of the predecessor of the section 6662(a) civil penalty and the section 7203 criminal penalty.

SEC. 8. EFFECT ON OTHER REVENUE PROCEDURES

Rev. Proc. 86-19 is superseded for taxable years beginning after December 31, 1991. However, if a taxpayer complies with this revenue procedure for prior taxable years, the taxpayer will be treated as having complied with Rev. Proc. 86-19 for those years.

SEC. 9. EFFECTIVE DATE

This revenue procedure is effective for taxable years beginning after December 31, 1991.

SEC. 10. EXAMINATION OFFICE CONTACT

All questions regarding this revenue procedure should be directed to the Office of the Assistant Commissioner (Examination). The telephone number for this office is (202) 566-6856 (not a toll-free number). Written questions should be addressed to:

Assistant Commissioner (Examination)

Attention: EX

Internal Revenue Service

1111 Constitution Ave., N.W.

Washington, D.C. 20224
Part Two:
Auditing EDI
Chapter 8.  

**Electronic Data Interchange — Effect on the Audit**

**Assessing Inherent Risk**

Because EDI will affect the nature of transactions entered into an entity’s accounting systems, including the initiation of transactions, its effect on financial statement assertions will be pervasive. The entire audit process from the understanding of accounting systems to the evidential matter used to substantiate transactions or account balances will be affected by the implementation of this technology.

Clearly one of the most important effects on the audit process is the elimination of paper documents that presently serve as an auditor’s major form of evidential matter, when testing controls or substantiating a transaction or account balance. Even more pervasive and potentially more difficult will be the auditor’s response to the new forms of business relationships and the profound effect on accounting systems and controls.

EDI can to some extent reduce the susceptibility of accounting applications to risk of misstatements because of procedures that must be put in place to conduct EDI with trading partners. The strict standards for formatting transactions, the significantly reduced data entry and reentry, the close relationship between trading partners, and the integration of operations between trading partners can reduce manual misstatements and identify how problems should be handled with predefined policies and procedures.

Conversely, implementation of EDI can increase management’s dependence on computer-based systems, potentially increasing inherent risk. Because EDI can increase the sophistication and complexity of an entity’s computer systems, it may be more difficult to implement management control methods that use data or other evidence that is external to, or independent from, the computerized systems.

Various factors can cause this increased dependence on computer systems. EDI implementation often results in new operational computer systems that produce accounting information as a by-product. Just-in-time inventory control systems or some of the interdependent relationships between entities for ordering inventory are examples of these operational systems. In many of these cases EDI is a necessary component to the implementation of such systems. These systems may make it difficult for management to independently establish methods that measure “actual performance” or “variances from expectations” (see Management Control Methods; AICPA Statement on Auditing Standards (SAS) No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit*, paragraph 6, Appendix A) when they are being produced or reported as by-products of the same systems used for operations.

In the past, these operational systems were manual or, if they were automated, they were on an independent computer system. Management could reconcile output from operational and accounting systems or compare them for reasonableness. EDI can facilitate the combining of these systems.
Other characteristics of EDI could also change the way management monitors its internal control structure. One such characteristic is the elimination not only of paper forms that document a business transaction, but also parts of the transaction itself. In the short existence of EDI, some entities have eliminated purchase orders and invoices.

In the retailing industry, some entities using EDI send stock status and sales information by location to their vendors. The vendors, based on this information and the planned inventory levels predefined by the retailer, ship the necessary quantities to replenish the retailer’s shelves. The retailer pays based on either the electronic shipping notice, usually sent when the vendor’s truck leaves the loading dock, or confirmation from the stores that the goods have been received. These electronic messages, substituting for an invoice, are valued and extended by the retailer, not the vendor. Price and shipping cost data and other terms are defined in their trading partner agreements and built into each of their computer applications.

In this example, it would be difficult for management to create effective detection controls external to the EDI computer applications. Control over the receipt of the goods may have to be accomplished by automatically reconciling actual receipt to anticipated receipts that come from the operational systems of the retailer or the vendor.

Monthly vendor statements may not be provided when two companies conduct business with EDI. Reconciliations are more apt to be performed by product line, season, or some other operational factor, eliminating the possibility of an externally generated control process based on the end of an accounting cycle, like a monthly accounts receivable statement.

For some entities on the leading edge of strategic EDI use, another issue exists when trading partners agree to different payment terms. These terms are used to create a motivation for a vendor to provide their product to a customer within very strict time commitments. One specific case, called “pay on production,” involves the purchaser paying for goods only after they are used in production, instead of upon receipt. Receiving information is now replaced with production information as the trigger to record a liability. Here is an example of the shift to use of an operational application for financial purposes.

“Pay on production” causes a loss of audit trail within the electronic documents that originated the transaction. This occurs because the liability is now being recorded as each individual item is used instead of a group of items that appeared on a line item of a purchase order and invoice. The customer’s accounting systems would be completely dependent on the operational system tracking the use of goods already received.

With “pay on production,” the vendor is dependent on the customer’s operational and accounting systems to provide information to allow recording of a sale. If these transactions are material to the vendor, the vendor’s auditors may need to consider whether the customer’s applications are part of the vendor’s applications and that some audit procedures may be necessary.

The issue of when title has passed should be detailed in the trading partner agreement. The agreement should also address which entity has risk of loss in relation to title passage.
The use of EDI will make computer applications more complex. The auditor may need to gain a detailed understanding of the relevant applications to obtain a sufficient understanding of the internal control structure. The following section outlines the approach that could be used to gain a detailed understanding of the application and the internal control structure.

**Control Policies and Procedures**

From a computer perspective, general controls cover the following functions:

- **Access**
- **Program Changes**
- **Application Controls**
- **Operations (minimal impact from EDI)**

**Access**

When an entity conducts business using EDI, controls over access to its computer systems take on added importance. Lack of controls over access to these computer systems could expose an entity to establishing unintended commitments with its customers and vendors that could not be easily voided.

EDI does not really change the nature of access controls needed, but increases their importance. Usage of security software or operating system security features and appropriate segregation of duties will be important.

As relationships evolve between trading partners, access to each other’s computer systems may become necessary. Access controls for third parties, such as trading partners, may take on increased importance.

A significant amount of time and effort could be required to identify and test these access controls. A more detailed understanding of the flow of transactions could be required to identify the critical data elements and program functions that should be protected by access software. Automated audit tools that can scan access control files and determine that access controls have been placed in operation may be required.

What an employee is authorized to do with the computer resources he or she has accessed must also have the same comprehensive level of control as access itself. Appropriateness of an individual’s access may need to be evaluated by review of privileges contained in security databases used by access security software and of the procedures for management authorization of privileges.

Authentication techniques (e.g., passwords or tokens) to assure that the requester is authorized access may be important. These techniques are typically contained in access software.

In an EDI environment access controls provide assurance that transactions are authorized. For the outbound transactions, controls over access and authorization to the application systems and programs could provide this assurance. The auditor may want to consider identifying and testing controls (to reduce control risk below the maximum) over access to this capability and data files.

As for inbound transactions, the communications software layer should have some way of identifying and authenticating authorized trading partners. Identifying an authorized trading partner is relatively easy. An EDI control database (Figure 8-1) could have an entry for all valid trading partners and their associated identification code and password.
Receiving a valid identification code gives Company B some, but not absolute, assurance that this is an authentic message from Company A. A password associated with the identification code, preferably sent in an encrypted form, could provide the necessary evidence that this transaction truly originated with Company A. A more elaborate authentication scheme would make the password dependent on the contents of the message, or important parts of it, which would also provide Company B with the assurance that the contents of the transaction had not been changed.

In practice, a password associated with a predefined list of authorized trading partners is the most common technique used. Only occasionally will the password be encrypted and rarely will that encryption be based on the contents of the message.

The auditor may want to test access controls over the file that contains the list of authorized trading partners and their associated passwords as well as the procedures for checking the list when a transaction is received. The latter procedure could be performed by any of the three software layers.

**Program Changes**

Virtually the same controls apply to program changes as to systems development with the added consideration of emergency or urgent fixes. The auditor may need to test controls over program changes to provide a basis for assessing control risk below the maximum.
Application Controls

Application controls should be present to prevent or detect misstatements that could cause material misstatements in the financial statement assertions. These controls can be directly related to the financial statement assertions:

- Completeness
- Existence
- Valuation
- Presentation

Rights & obligations (covered by discussion on completeness and existence)

Completeness. In an EDI environment application controls can be built into any or all of the three levels of software to assure that all transactions are complete. In a more traditional computer application, the classic “batch total” control procedure would be designed to meet this control objective. However for an EDI environment this control must be established by the program when the transaction is initiated or received.

For an outbound transaction this control objective could be satisfied with entries into an EDI control database, (see Figure 8–1) or some other control files or techniques, when the transaction is successfully processed through each of the three levels of software. The entries should contain cross-references which identify the transaction as it changes from the proprietary format of the application programs to the EDI standard format, and finally as a portion of a long message train.

For an inbound transaction the entries are made in the opposite order and must be either cross-referenced as a response to an outbound transaction or entered as a new transaction requiring matching entries starting with the application software.

The unmatched entries in the EDI control database should be aged and those that are not reconciled with matching transaction sets should be investigated after some specified period. This specified period could vary by each transaction, dependent on parameters in the initial transaction. For example, an EDI purchase order may contain a specified delivery date. The purchase order acknowledgment and other responses from the trading partner should be received before that date. The purchase order could have more than one date, i.e., one date to anticipate the acknowledgment and another for the shipping notice and still another for receipt of the invoice.

Electronic techniques in the communications layer determine that each EDI transaction is complete. This successful processing is typically logged into the EDI control database. Most communication protocols include algorithms for predetermined values for a check digit. These techniques can identify if any “noise” or loss of signal altered the data in the transmission and automatically request retransmission. These techniques are very similar to parity checking for information written to or read from a computer’s internal memory. The auditor may want to determine if these types of controls were in effect for the audit period.

At the EDI translation level, the software packages generate a functional acknowledgment for transactions received. The functional acknowledgment indicates that all of the EDI data segments and transaction set headers and trailers are correctly represented according to the EDI standard in use. An entry should be made in the EDI control database that an outbound transaction was understood by the trading partners’ EDI translation software as evidenced by receipt of a functional acknowledgment. The functional acknowledgment is merely a safeguard that both parties’ EDI software will understand the data elements in the transac-
tion and will be able to pass them on to the application software where a decision regarding the nature of the transaction can be made. The functional acknowledgment does not give the sender any sign-off or acceptance about the contents or a requested commitment contained in the purchase order.

If the auditor wishes to assess control risk below the maximum, the auditor may need a detailed understanding of how the client tracks EDI transactions through its software layers and what reconciliation procedures are performed by the application software, or perhaps by special control programs that analyze the EDI control database, other control files or techniques. A detailed understanding of the flow of transactions through the layers may also be required.

An EDI control database could help to provide assurance that transactions were recorded in the appropriate accounting period. The different levels of acknowledgments between the trading partners need to be defined and the concept of a complete portfolio of transaction sets must also be discussed.

Existence. The functional acknowledgment, discussed above, offers Company B only limited assurance that the transaction sent to Company A was understood per the agreed-upon standards. A separate EDI transaction acknowledging acceptance of the contents of the purchase order and any implied commitments is required before Company B can be satisfied that their operational needs, which caused the initiation of the purchase order, can be met by Company A. Note here that the purchase order and the acknowledgment may have contained data segments as to required delivery schedules or shipping terms that could represent a legal contract between Company A and B.

A liability does not exist until the goods are shipped or received, depending on the trading partners' agreement and the shipping terms expressed in the purchase order and agreed to in an acknowledgment transaction. The EDI control database may indicate that a liability should be recorded when it is updated with information entered from Company B's receiving department, or the liability may be incurred when Company B receives an electronic shipping notice from Company A or an electronic manifest from a freight company — i.e., FOB shipping point. Therefore, the necessary portfolio of EDI transaction sets required to record a liability and the timing of the liability may vary based on the terms in the EDI transactions.

The trigger point for recording a transaction may be different for various vendors of Company B and must be controlled by tracking the status of these transactions in an EDI control database where all of the appropriate information can be processed by the application software layer. An aging and analysis prepared from the incomplete portfolios of entries in the EDI control database could assist in controlling the assertion of existence at the audit date. A well-designed accounts payable system may also include the electronic bill of lading to verify the shipping date. In the retailing industry it is fairly common that the liability is recorded when the electronic bill of lading is received from the shipper. The retailer then uses the shipping information for receipt priority planning to assure efficient distribution.

The auditor may want to determine the shipping terms used and determine if the procedures contained in the applications provide for appropriate correlation of dates to enable recording of transactions on a timely basis. Review of the aging of incomplete portfolios or perhaps reconciliations of complete transaction portfolios and bills of lading could provide some assurance over the timely recording of transactions.

Valuation. In many cases Company B's trading partners may send priced and extended electronic invoices which can be logged into the EDI control database and recorded in the general ledger by the application software layer. In these
cases the controls assuring completeness could assist in determining proper valuation if a comparison to the purchase order price is performed. Also, access controls over the price file used when the purchase order was created would have to be considered.

However, as relationships between trading partners evolve, the trend is to remove redundant transactions, such as the electronic invoice. In this case the shipping notice or the receiving information is valued by Company B itself, not Company A. In this case access controls and authorization to change the prices associated with the trading partners’ products are the primary form of assurance that the accounts are properly valued.

In some cases Company B may allow Company A to electronically review the prices Company B is using. Company A may send electronic price catalogues that Company B can use to update the prices. The review and authorization for these periodic price catalogues must also be controlled by Company B’s access and authorization software; these may need to be addressed by the auditor.

Presentation. In a non-EDI environment, entities often have invoices with a stamped stencil allowing clerks to write general ledger account numbers to support the distribution. Since invoices are not used in many EDI environments, this classification is instead included in the electronic transaction and is by design a programmed control procedure. Control over presentation could occur based on the nature of the product being purchased or sold. Association with a vendor, a part number, or the initial electronic purchase order could also determine if it is classified as inventory, fixed asset, or expense.

**Tests of Controls**

The nature of tests of general computer controls should not differ greatly from those being performed in audits where EDI is not a significant factor since the nature of these controls is not affected by EDI. However, the extent of test work on these controls may increase because of the importance of these controls in an EDI environment.

Application controls will change in nature as described above. They will become a part of the computer processing. They will replace or provide most of the data for external detective controls. The auditor may need a detailed understanding of how these controls function to identify potential evidence that would provide assurance they were operating effectively during the year. This evidence may be electronic and some of the procedures identified in the following section on designing substantive procedures may need to be applied to test these controls effectively.

**Assessing Control Risk**

An entity’s internal control structure consists of the policies and procedures established to provide reasonable assurance that specific entity objectives will be achieved. Although the internal control structure may include a wide variety of objectives and related policies and procedures, only some of these may be relevant to an audit of the entity’s financial statements. Due to the nature of EDI, certain control procedures that used to be performed manually may have to be replaced with automated control procedures.

As EDI evolves and becomes more pervasive, the predominant way for management to control their business could become the establishment of controls over the development and maintenance of the computer systems they are making themselves dependent upon. Further, management may have to define in great detail their control functions during system design and not on a retroactive basis.
Once application controls are built into the computer application, they may become the primary means of protecting assets and assuring accurate financial reporting. If this development process is not controlled and the resulting computer systems are not safeguarded from inappropriate use or access, management’s ability to control their operations may be compromised and control risk may be increased.

**Designing Substantive Audit Procedures**

The auditor uses the knowledge provided by the understanding of the internal control structure and the assessed level of control risk in determining the nature, timing, and extent of substantive tests.

Substantive testing is the area where EDI creates the most challenges and potentially the most benefits to the audit process. When evidential matter can be obtained from independent sources outside an entity, it provides greater assurance of reliability for the purposes of an independent audit than that secured solely within the entity. In other words, while auditing Company B in Figure 8-2, the auditor should examine the documentation that proves that the evidence came from outside Company B and was independent of Company B’s systems and internal control structure policies and procedures. Historically, this would equate to paper invoices with company logos, or bills of lading associated with the receipt of goods documented on an invoice. But in the EDI environment these items are electronic records that could be created by any computer.

![EDI Electronic Evidence Diagram](image-url)  
*Figure 8-2*
The auditor may want to examine how an EDI transaction is evidenced in its flow through the trading partners' computer systems and any intermediary systems like a VAN. Identifying the different places the evidence exists may provide the auditor with the evidential matter necessary to support the auditor's conclusion. As will be discussed later, adding some additional electronic documentation within the EDI messages themselves may also provide the substantiation needed.

Using Figure 8-2 again, follow the flow of an EDI transaction through the system layers and identify where evidential matter may exist. If Company B is the auditor's client and Company A is sending the client an invoice there are seven places where the EDI transaction may be evidenced.

1. Company A's MIS applications. This would be their sales or billing system. The record generated would be in a format proprietary to Company A's application systems and would not exist in an industry standard form that could be understood by Company B.

2. Company A's EDI translation systems. The invoice would exist on the files maintained in this system and would be in a format that Company B, or more importantly Company B's auditors, could understand.

3. Company A's communications system. The invoice, along with other invoices and other EDI documents sent to Company B (and EDI documents sent to other Company A trading partners) would exist on log files. They would be stored in a standard format inside of a double electronic envelope as described in the Appendix of Chapter 1. The outside envelope would be the Communications Transport Protocol and the inside envelope would be the Interchange Envelope, in this case identifying Company B.

4. If the VAN maintained logs of transactions between Company A and B the invoice in the standard format would exist on files maintained by the VAN. The format of these records would of course be the standard, unless the VAN was translating from one standard to another for the two trading partners. The Interchange Envelope would also be wrapped around the EDI transactions headed for Company B along with the subject invoice.

5. Company B's communication system. The invoice would be found in the same format and enclosures as described in Company A's communication system except for the transactions for Company A's other trading partners.

6. The transaction would exist in the standard format on files maintained by Company B's EDI translation system.

7. Finally, the invoice would be written to Company B's accounts payable file in their proprietary format created by the accounts payable or purchasing application.

The external quality of these new forms of electronic evidence provides potential for some new substantive procedures. A further description and analysis of their audit quality will be discussed in the Appendix to this chapter.
There are several areas where the auditor may want to concentrate his or her efforts in making recommendations to clients using EDI.

- **General Computer Controls** — Because of the increased importance of this control area the auditor may want to urge the client to apply tight tolerances to compliance with comprehensive controls.

- **Involvement in Systems Development** — The auditor may comment on the extent of involvement by management in the development of computer applications, especially programmed control procedures which management will use to control not only their financial information but also their operations.

- **Trading Partner Agreements** — The auditor may review and comment on whether the trading partner agreements are consistent with the control procedures identified during the audit. Are the terms of the agreement consistent with the initiation of a transaction and the controls over existence and completeness?

- **Value Added Networks** — The auditor may review and comment on whether the VAN represents a significant portion of the client’s accounting applications, and consider if a third party review may be required.

Increased dependence on computer systems for operations and financial records should justify appropriate control considerations for protecting the company’s ability to continue to do business. Off-site storage, hot sites, and testing of recovery and backup procedures should become normal business practices in an EDI environment.

**Summary**

Auditors should consider obtaining and documenting a detailed understanding of the client’s applications systems when EDI is used. EDI will cause increased system complexity and management dependency that may require this level of understanding to effectively and efficiently design audit procedures. Auditors should consider determining if the use of EDI has changed the business processes and determine the appropriate effect on the audit.
Perhaps the new forms of evidential matter in EDI systems could allow the auditor to reperform the processing of most of the evidential matter supporting the amounts in Company B's financial statements. This would provide the auditor with a high level of assurance that the financial statements are fairly presented. This could be very beneficial if Company B was not very conscientious about implementing an EDI control database or some other type of file tracking. Also, it could be important in those situations where classic alternative procedures need to be applied, like examination of bills of lading or shipping documents.

Naturally the cost of performing these procedures must be weighed against the audit benefit and the assessment of risk already identified. These procedures could be very costly. In fact, at the present time, they are rarely being applied. Therefore, in addition to describing how these potential substantive procedures would work, their pros and cons will be discussed as well.

The invention of powerful cost-effective audit retrieval systems and the dramatic decreases in computing costs enabled auditors to begin manipulating computer files to fulfill audit objectives. Use of common EDI standards, translation software and VANs are among many other factors that may cause these potential computer assisted audit procedures to become cost justified.

**Historical Electronic Confirmation**

The auditor would send requests to Company B's trading partners for transactions that he or she is interested in verifying. In the case of EDI however, the request to Company A could be for all of Company B's EDI transactions both sent and received for the period under audit. As Figure 8–3 indicates, the auditor would probably ask for the records stored in Company A's EDI translation systems. Transactions in the MIS systems would not be in a standard format and in the communication system they would be mingled with EDI transactions for other trading partners. Note that in the diagrams the dark arrows identify movement of information for the audit process while the light arrows identify the normal EDI information flow.

These transactions could be transmitted directly to the auditors or they could be sent on a magnetic tape. If Company A retains these records for the period of the audit, it should be very easy for them to select the transactions to meet the confirmation request.

The next step will be to match the transactions received from Company A with the EDI transactions in Company B's EDI translation software layer. The formats should be the same; in fact, there should be a perfect one-for-one match. Note that the quality of the external evidence is very high. The auditor has received these transactions for testing directly from Company A and completely independent from Company B's computer systems or internal control structure.

Matching is performed by a Computer Assisted Audit Technique (CAAT) which is processed independent of Company B.
One additional step that is required is to trace the EDI transactions into the files that directly support Company B’s financial statements.

The major potential problems are:

- Company A might not wish to supply tapes of all transactions to all its trading partners’ auditors.
- Different trading partners may use different “standards” and these may vary over time.
- Tapes supplied by Company A may contain duplicates owing to retransmission where errors have occurred.
- Company A might only retain transactions on its MIS applications.
- The final step of vouching the confirmed transactions from Company B’s EDI translation system to the files in the MIS applications may have to be done on a test basis depending on cross-referencing between the two system layers.

**Auditor Transaction Sets**

For auditor transaction sets, the auditor might use his or her own set of ANSI X12 (or other accepted standards) to independently request an electronic confirmation of a specific transaction from one of Company B’s trading partners. If a purchase order is coded as an “82N,” then perhaps the auditor would send an “82X” with the selected purchase order attached to Company A — assuming
that is where it went originally. Company A receiving the “82X” would be asked to interrogate their files and respond with an “82Y” — yes we received that purchase order — or an “82Z” — no we did not receive that purchase order or an “82W” with his or her version of the purchase order if there was a difference in the data. Similar auditor transaction sets could be used to confirm other electronic documents.

Figure 8-4 depicts the auditor using the client link to the EDI network for transmission of the auditor transaction set. It also shows that the transaction was selected from the MIS application software layer to eliminate the final vouching step that was required in the historical electronic confirmation technique. In this scenario the auditor is using the client’s EDI translator system also. Some procedures to provide control of processing these auditor transactions would be needed similar to the processing control procedures performed for a CAAT processed on the client’s computer.

Figure 8-5 depicts the auditor as having his or her own link to the EDI network and EDI translation software. This scenario would not require the control of processing procedures and would be less disruptive. Both of these approaches could be performed continuously throughout the year or on an historical basis at a point in time. A characteristic that all of these substantive procedures have in common is the high quality of the evidence they produce. The verification of the contents of the transaction comes from an entity completely independent from Company B.
The potential problems associated with this approach are:

- Significant systems enhancements would be required to uniformly respond to the new auditor EDI transaction sets. The new transaction set would need to be created and adopted by the trading partners, which may be burdensome.
- The audit request may have to be sent on a current basis to avoid confirming transactions that were several months or even a year old.

**Dynamic Confirmations**

As depicted in Figure 8–6, this technique offers as high a quality of external evidence as the others and appears to have the least cost or overhead associated with it. The VAN may be willing, for a minimal fee, to direct transactions between one company and its trading partners to the auditor, either as they occur, or for a specified period. Knowing in advance which of its customers require this service could prevent saving or logging all transactions in mass and then searching for them based on a subsequent request.

Also, if this store and forwarding operation is still too expensive for all transactions, a sample may provide the evidence needed by the auditor.
Depending on the VAN’s abilities and flexibility, the auditor has several options in structuring tests with this approach. The auditor could:

- Take all of the appropriate transactions for the period under audit directly from Company B’s MIS application layer and match them against all of the transactions processed by the VAN for the same period. This would require an EDI translation step.
- Take a sample of transactions from Company B’s MIS application layer, translate them into EDI standard format and request only these from the VAN.
- Take a sample of the transactions provided by the VAN, translate them from EDI standard formats and match the sample with transactions from Company B’s MIS application layer.

About the only potential problems with the dynamic confirmation technique are that the trading partners may not use VANs or the VAN may not be willing to provide the service at a feasible fee.

It is not too difficult to imagine that, regardless of the extent of services provided by the VANs, auditors may need third-party reports evaluating the controls over the VANs operations that affect their client’s accounting systems, especially these services which affect the auditor directly.
Electronic Signatures

It may be possible to obtain external evidence from Company B’s MIS system without involving independent trading partners or VANs directly, if an “authentication” system is used. Such a system effectively provides an “electronic signature” that cannot be tampered with (this is explained further below). The verification by an auditor of the authenticity of this signature would provide the necessary external evidence to satisfy any audit procedures. One could therefore read through the data (with a CAAT) and total all purchases from each supplier.

Figure 8–7 illustrates the simplicity of this approach relative to the others. The public keys, which are explained further below, are used to determine that the signature contained in the transaction was created by the entity associated with the public key and that particular transaction. The public key matching the electronic signature and the contents of the transaction gives the auditor the evidential matter necessary to support the auditor’s conclusion. If the electronic signature and EDI record remain intact on each transaction when passed from Company B’s EDI systems to its MIS systems, the auditor may be able to verify records that directly support Company B’s financial statements.

The major potential problems with this are:

- Such an authentication system may not be used in a given industry due to cost considerations.
- The data may be purged regularly and thus may not be available.
There may be different electronic signature standards for different suppliers, varying over time.

The authentication system uses what is known as “public key” encryption. This can be used either to encrypt data (make it private) or to authenticate it (sign it). It works as follows. Each entity has a pair of “keys” (numbers), one private key (known only to the originating entity’s system) and one public (like a telephone number). Assume Company A wants to send an authenticated message to Company B. A encrypts the message using its private key.

The keys are designed such that the encrypted message can be decrypted using A’s unique public key (which is of course known to B). Thus B, and B’s auditor, knows that the message came from A. Unfortunately, for this to work securely, the key numbers have to be quite long, so a considerable processing overhead is needed, which makes it expensive. This can be reduced in EDI transactions by only encrypting a hash total of important fields in the message.

As a matter of interest encryption for privacy (as opposed to authentication) works the other way round. For A to send a private message to B, the message must be encrypted using B’s public key. B decrypts it using his or her own private key. From this, one can see that the authenticated messages received by B could be a valuable source of external evidence to the auditor.

**Combined Approach**

Another alternative that would not involve cooperation from third parties would be to use the log file created by the communications software layer (see Figure 8–8). This file would need some reformatting to “open” the communications envelopes and to separate and sort the EDI transactions out of the different functional groups into a homogeneous file of matching transaction sets. Because of the standardization used this complicated step should still be feasible.

One important piece of information in this process would be the identification code and perhaps password of the sender. This information would be contained in the “Interchange Control Header” (see the Appendix of Chapter 1) and could be tagged onto all the associated transactions. This piece of information, once it is compared to the authorized trading partner file, would provide the external evidential quality the auditor requires.
The next step as indicated in Figure 8–8 would be to match all or a sample of these transactions to the files in the MIS layer of the software.

The title of this technique refers to the necessary existence and testing of internal control structure policies and procedures contained in the communication layer. Most important would be the access controls over the communication programs and the log files used for the audit test.

The major potential problems with this technique are:

- The data may be purged regularly and thus may not be available.
- The access controls may not be adequate to support an assessment of control risk below the maximum.
References


*EDI Forum*, EDI Publications, Inc.


Bibliography


Competitive Ledge, The 1990 EDI Sourcebook.


EDI Forum, EDI Publications, Inc.


EDI Monthly Report, Congressional Information Bureau, Inc.


123
EDI, Spread the Word!, EDI Yellow Pages — International, Dallas, Texas, 1992.


S. Kerr, EDI Legal Laissez Faire, Datamation, April 15, 1989.
Bibliography


EDI Control, Management, and Audit Issues


Glossary

Access Control
Access control is a component of logical security which itself should be seen as a continuum covering the whole computing platform from systems to applications and related data, including communications, networks, servers and utilities. Specifically, access control refers to limiting access to the computing environment resources only to those having either ownership rights or the right to use. This is a key area of control and must be consistent and seamless with change control management practices.

Algorithm
A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

Analog
Transmission method that carries intelligence in the form of data, voice, sound and images using variable wave patterns.

ANSI
American National Standards Institute: developer of the ANSI X12 generic EDI standards. The ANSI Accredited Standards Committee – EDI publishes Standards for EDI in the U.S. The Canadian Standards for Inter-Financial EDI are based on ANSI X12.

Auditability
A characteristic (attribute) of information which exists in the context of modern information system when it can be substantiated by tracing it to source documents, or when reliance can be placed upon pre-verified and continually monitored control processes.

Authentication
The verification of the source, uniqueness, and integrity of a message.

Business Process Reengineering (BPR)
Modern expression for Organizational Development stemming from IS/IT impacts. The ultimate goal of BPR is to yield a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings. To reengineer means redesigning a structure and procedures with intelligence and skills and be well informed about all of the attendant factors of a given situation, to obtain the maximum benefits from mechanization as basic rationale.
Canadian Payments Association (CPA)

The federally regulated organization charged with the planning, development, and administration of the Canadian payments system. This function includes the national clearing and settlement system, both paper-based and electronic.

Challenge and Response

A form of extended user authentication. After entering an ID and password, the user is issued a challenge by the system which must be responded to. When the user's response is received, the system compares it with the computed response. If they match, the user is allowed access to the system. The system issues a different challenge every time and therefore requires a new response each time. The response to a particular challenge will be different for every individual. In effect, a new password is used in every logon.

Change Control

This is part of the operations and a critical area of control. Change control is a process composed of structures, procedures, documentation, and access control having to do with library control and management over program changes in the production environment. Change control involves both application program changes as well as systems changes and is subject to review at any time by auditors to provide assurance that the policies, methods and procedures prevent unauthorized access to object code and execution libraries, that all the changes are properly logged, approved, authorized, documented, and properly scheduled. It includes adequate segregation of duties and sufficient checks and balances to prevent accidental or willful injury to the computing environment, while leaving a sound trail of all related steps and procedures over several generations of changes. In modern computing environments, change control can be engineered to meet all the key control criteria.

Check Digit Verification

A programmed edit check where an extra digit is included to a piece of data like a customer number, vendor number, or part number. Using a routine the computer checks the validity of the incoming data.

Ciphertext

Encrypted (enciphered) data, which may be stored and transmitted in a non-readable format.

Compliance Program

A means of periodically reporting conformity to mutually agreed upon standards of control and audit by two or more parties in an EDI system over a specified period of time. Any exceptions are briefly noted with corrective action implemented or planned according to operating rules. Management produces a Statement of Compliance to agreed upon standards of control and the auditor reports an independent and objectively determined Statement of Opinion on management's statement.
Computer Aided Software Engineering (CASE)

The rationale of CASE can be simply described as, an attempt to mechanize the mechanization process. The approach is, using appropriate systems tools, designers in upper CASE, define entities, relationships, dependencies and so on, and if this is done properly, in lower CASE the systems will be coded automatically. Objectives are to speed up development and ease the enhancement and maintenance burden.

Computer Virus

It is an unwanted piece of software, specifically designed by its programmer, to destroy, damage, disturb, disrupt, or nag. It affects adversely, data, the computing platform, and the users. For a virus to be a virus it must meet the following characteristics. It is a piece of software, which executes according to a prespecified trigger, like a date, an event, or sequence. It has the ability to move from environment to environment by attaching to data moving over networks. Then, the system is known to be infected and in turn will infect the other unprotected resources which are in communication with it exchanging data. It replicates itself, lying dormant until the trigger executes it. Problems can go from mere nagging situations with flashing unexpected messages on the screen, all the way to complete destruction and scrambling of the data on mass storage devices, by destroying file allocation tables, poke holes and break chains. Countervailing procedures must be enacted to prevent, detect, and correct for viruses. Bulletin boards and universities are famous breeding grounds for computing viruses. The more knowledgeable the designer regarding the computing architecture the more vicious the viruses that can be designed. The worst scenario is when all backups have been infected with an unknown virus which suddenly executes to damage the environment.

Console Logs

It is a control whereby all actions taken by an operator are logged automatically. Jobs executed, terminations, and any activity performed by the operator is recorded.

Control Data

This is the data raised on the performance and behavior of controls. There should be no restriction on the generality of this definition. However, in general terms it refers mostly to the data flowing from monitoring systems.

Control Objectives

With respect to information, these are accuracy and completeness, security (including authorization), auditability, timeliness and recoverability.

Control Structure

The internal control structure of an organization consisting of the policies and procedures established to provide reasonable assurance that its objectives will be achieved. There are three basic components to the control structure: the control environment, the accounting system, and the control procedures. From an accountability perspective there are two premises underlying the control structure, the first is management responsibility and the second is reasonable assurance.
Cryptographic Equipment
Hardware that performs cryptographic functions, e.g., Encryption, Authentication, Key generation.

Cryptographic Key
A parameter that determines the transformation from plaintext to ciphertext or vice versa.

Cryptographic Service Message (CSM)
A message for transporting keys or related information to control a keying relationship.

Data Element
The smallest named item in each transaction set. Together with a segment ID and other data elements, they form data segments. A data element can represent a qualifier, a value, or text such as a description.

Data Encryption Algorithm (DEA)
The cryptographic algorithm specified by ANSI X3.92. DEA is also referred to as Data Encryption Standard (DES) in the U.S.

Data Key
A working key used to encrypt and decrypt or to authenticate data.

Data Segment
Subsections of data into which each transaction set is divided, composed of a segment ID and a fixed number of functionally-related Data Elements.

Decryption
The process of transforming ciphertext into plaintext.

Dependency Check
It is a programmed edit routine testing whether the contents of two or more data elements or fields within a transaction bear the correct logical relationship.

Digital Signature
Sometimes called electronic signature, is an electronically generated, digitized (as opposed to graphic which is done by hand) authorization uniquely linkable and traceable to a specifically empowered officer. It is a number, essentially a checksum added to a message to accomplish the required services.

Double Electronic Envelope
An electronic message bracketed by header and trailer records for the Communications Transport Protocol and also header and trailer records for the Interchange Envelope. See Interchange Envelope for further definition.
Dual Control
A process of utilizing two or more separate entities, usually persons, operating in concert, to protect sensitive functions or information. Both entities are equally and separately responsible for the physical protection of materials involved in vulnerable transactions, such that no single person shall be able to access or utilize the materials.

Dual Read Check
A hardware control where records are read twice to ensure that the data is read correctly.

Echo Check
The CPU sends a signal to a peripheral device which returns it to the CPU to verify proper functioning.

EDI Transmission
A Functional Group of one or more EDI Transactions sent to the same location, in the same physical transmission, identified by a Functional Group header and trailer.

EDIFACT
EDI for Administration, Commerce and Trade, refers to the EDI standards being established by the United Nations Economic Commission for Europe.

EFT
Electronic Funds Transfer: Information passed between banks or other financial institutions which results in debits and credits, i.e., value transfer. Examples are wire transfer, American Clearing House or Canadian Payments Association debit. It carries very limited payments information.

Electronic Commerce (EC)
Those are other means of electronic transmission which do not involve standard formats, or necessarily computer to computer exchanges in terms of computer application job streams. Examples are: fax, bar coding, public E-mail like the Internet, videotext, processing documents using proprietary formats, bulletin boards (BBS), and others.

Electronic Data Interchange (EDI)
The electronic exchange of data between organizations, in a structured computer processable message format, using public or industry standards. Examples are purchase order, invoice, payment and remittance advice.

Electronic Security Module (ESM)
See Hardware Security Module.
Embedded Audit Module (EAM)
Programming which has been added to system software which permits monitoring or testing of controls or audit procedures. As an automatic monitoring device it may monitor integrity controls, for authorization, accuracy, security, authentication, encryption, and detect and report to the auditor, where applicable, their failure to perform as required.

Encryption
Process transforming plaintext into ciphertext which is unintelligible to the human eye.

Envelope
A header and trailer record, attached to the front and back respectively, of a set of data, usually a message. The purpose is usually to direct the message to an address and to provide assurance that the data was not changed during transmission.

Exclusive or Combination Method
A method of combining key components manually to initiate a keying relationship.

Expert System (ES)
It is an information system that emulates the problem-solving techniques of human experts, in subject specific applications, like medicine, geology and so on.

FEDI
Financial EDI is information passed between financial institutions and companies that relates directly to payments and payments-related data. At the option of the payer, the remittance information can be collected, analyzed and reported back to the payer as specified, thus compressing the reconciliation cycle and unloading some of the accounts payable functions. Examples are: payment order, balance inquiry, bank statement, deposit notice, remittance advice.

File Server
A file server is a resource normally found associated with networks representing mass storage for data and software.

Functional Group
One or more similar transaction sets exchanged between partners in a single transmission. Example: A group of purchase order related transaction sets would be a functional group. A functional acknowledgment is an electronic confirmation of receipt of such a message.

Function Group Header and Trailer
A header and trailer record, attached to the front and back, respectively, of one or more EDI transactions of the same type, like invoice, purchase order and so on.
**Gateway**
Link, bridging two different networks which provides seamless processing between computing platforms. It is a connectivity term.

**Hardware Security Module (HSM)**
It is a self-contained, physically secure, special purpose computer that performs security-related processes and stores security parameters and/or other sensitive data.

**Header Record**
A record attached to the front of a group of computer records that contains information relevant to that group of records.

**Information Center**
This is basically an organizational staff unit designed to enhance end user computing (EUC), assist, coordinate, and support the users. Corporate policies and control plans must be enacted to insure compliance with acceptable practices.

**Integrated Services Digital Network (ISDN)**
A public network for multimedia transmission. Voice, image, data, sound and so on. The impact over time will be to converge applications and devices to digital based technology. Analog devices like radios, TV and so on would be designed to operate in that mode.

**Integrity Controls**
Those manual or programmed controls whose purpose is to ensure that the objectives of accuracy, completeness, security and confidentiality of data during input, processing, output and storage are met.

**Interchange Envelope**
See Interchange Header and Trailer.

**Interchange Header and Trailer**
The header and trailer records, attached to the front and back, respectively, of a group of EDI transactions going to the same trading partner. Example: all of the purchase orders in a transmission from Company A to Company B.

**Key Custodian**
The persons, assigned by the security administrator of the trading partner, given the responsibility of either sending or receiving a component of either the master key or key exchange key used to encrypt data encryption keys. The control technique here is dual control with split knowledge which requires two key custodians.

**Key Encryption Key**
Normally referenced as KPE is a key used exclusively to encrypt/decrypt keys, also known as data key or working key.
Key Exchange Key (KEK)
Is used to protect other keys, either other key encryption keys or data keys, during an exchange between two parties.

Key Material
The data necessary to establish and maintain cryptographic keying relationships.

Keying Relationship
The state existing between trading partners and/or financial institutions in which they share at least one cryptographic key.

Mailbox
An electronic facility into which a trading party deposits business documents for distribution to one or more receiving parties who can subsequently store or retrieve the documents at their own convenience.

Mapping
Converting data from an organization’s internal format to standard format.

Master Key
The encryption key used to encrypt key encryption keys and data keys during their period of storage on file.

Message Authentication Code (MAC)
A cryptographically computed value that is the result of passing data through the authentication algorithm using a specific key. MAC can be used as a hash total or control total when data must be protected from alteration.

Object Oriented Programming (OOP)
This approach treats the organizational units as entities with relationships between them, and how they interact. The major advantage is that objects are reusable. It is like developing a series of building blocks which can later be used in various ways and combinations. It is faster and easier than developing each application from scratch.

Open Systems

Payment Data
The portion of the Financial EDI transaction which is directly related to payment. It includes items such as identity of creditor and debtor, transaction value, value date, and date of message origination.
Physically Secure Device
A device designed to preclude successful penetration to reveal all or part of any cryptographic within the device. The art of successfully penetrating the device must cause any cryptographic key stored within to be erased or rendered unusable. Successful penetration must require specialized skills, equipment and facilities not generally available. The device must be designed such that any tampering will produce noticeable damage.

Plaintext
Unencrypted data: intelligible data that can be directly acted upon without decryption. An example is an ordinary ASCII text file.

Pre-Verification of Controls
In the on-line, real-time data processing environment, it refers to the on-line real-time testing of controls such as user identification codes, user authorization profiles, terminal source, message authenticity and encryption.

Programmed Control
Control performed by the computer. It can be application, systems, and process.

Prototyping
In environments using state-of-the-art technology, prototyping represents a quick way to get a handle on development of applications. It is highly interactive with the user to establish functionality, then derive the full specs and development.

Recoverability
The control objective of recoverability in the context of EDI is to ensure that in the event of a failed transaction set or system outage, recovery is obtained within a mutually acceptable time frame, through adequate backup, retention and contingency plans.

Remittance
Other data transmitted in a Financial EDI transaction except payment data. It includes supporting documentation such as purchase orders, invoice stubs, and invoice numbers.

SAS
Statement of Auditing Standards, issued by the AICPA.

Security
The control objective of security is to ensure that all EDI related software and data defined as confidential are adequately protected against unauthorized disclosure or change during storage or transmission, and that physical access to equipment is restricted.
Security Related Incidents (Security Incidents)
Incidents related to the security of Financial EDI, which may include: MAC verification failure; Cryptographic Service Message counter out of sequence; known or suspected compromise during the manual key distribution process; known or suspected penetration of a physically secure device; known or suspected compromise of a key.

Split Knowledge
A condition under which two or more parties separately have key components that individually convey no knowledge of the resultant cryptographic key.

TDCC
Transportation Data Coordination Committee, which developed and published the first set of EDI standards in the U.S.

Third Party Network Provider
Also known as Value Added Network (VAN) provider or Intermediate Network Connector, is a service bureau supplier of communications facilities including translation software and integrity controls to trading partners and financial institutions in an EDI network.

Totally Systems Dependent (TSD)
This describes a condition whereby an organization is completely paralysed if systems are down. Substantial losses are sustained even if down for a short period of time. It also refers to situations where an auditor has no acceptable alternative to relying on systems.

Tracing Request
A request for information on location/routing of a specific EDI transaction for purposes of resolving problems between trading partners.

Trading Partners
Organizations engaging in EDI. Includes the originator and the receiver.

Trading Partner Agreements (TPA)
A written contract between two trading partners wishing to conduct business using EDI. The agreement describes how the partners will interact electronically, the EDI transaction types that will be used, which EDI standards will be followed and other communications concerns such as protocols and frequency of connections.

Transaction Reference Number
Unique number, to be contained in each EDI transaction identifying that EDI transaction.
Transaction Set

One complete business transaction, corresponding to a business transaction which would normally be exchanged between trading partners. Several related transaction sets may be placed into a functional group.

Translation Software

The process whereby the EDI Software translates incoming documents or flat files into a format which the receiving party wishes to receive. The EDI format is either an industry standard like TDCC, UCS, and WINS, or a public standard like ANSI X12 and EDIFACT.

UCS

Uniform Communication Standard — used by the grocery industry.

Value Added Bank (VAB)

This describes a bank which offers the services of a VAN along with the payments capability of financial EDI (FEDI).

Value Chains

Linkages created with suppliers who furnish goods and services which add value to a company’s product or service. A value chain includes all of the goods and services from raw material to the product. It can be extended to include value added services provided by third party network suppliers and the paying agencies.

VAN

A Value Added Network is a third party which provides communications switching and other value added services between trading partners. Those services are EDI translation services, conversion from one EDI standard to another, message control reporting, authentication, electronic mail box services for notification of receipt of messages, line speed matching and so on.

Vendor Agreements

Agreements written by the counsel of vendors of third party network service providers or EDI software suppliers to maximize the vendor’s rights and minimize the vendor’s exposure to liability.
Abbreviations Used

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4GL</td>
<td>Fourth Generation Language</td>
</tr>
<tr>
<td>ABA</td>
<td>American Bar Association</td>
</tr>
<tr>
<td>ACH</td>
<td>Automated Clearing House</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AICPA</td>
<td>American Institute of Certified Public Accountants</td>
</tr>
<tr>
<td>AIS</td>
<td>Accounting Information Systems</td>
</tr>
<tr>
<td>ANA</td>
<td>Article Number Association</td>
</tr>
<tr>
<td>ANS</td>
<td>American National Standards</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>ASC</td>
<td>Accredited Standards Committee</td>
</tr>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ASII</td>
<td>Application Seamless Integration</td>
</tr>
<tr>
<td>ASM</td>
<td>Association for Systems Management</td>
</tr>
<tr>
<td>BPR</td>
<td>Business Process Reengineering</td>
</tr>
<tr>
<td>CA</td>
<td>Chartered Accountant</td>
</tr>
<tr>
<td>CAAT</td>
<td>Computer Assisted Audit Techniques</td>
</tr>
<tr>
<td>CAD</td>
<td>Computer Aided Design</td>
</tr>
<tr>
<td>CAM</td>
<td>Computer Aided Manufacturing</td>
</tr>
<tr>
<td>CASE</td>
<td>Computer Aided Software Engineering</td>
</tr>
<tr>
<td>CBA</td>
<td>Certified Banking Auditor</td>
</tr>
<tr>
<td>CBA</td>
<td>Cost Benefit Analysis</td>
</tr>
<tr>
<td>CBIS</td>
<td>Computer Based Information Systems</td>
</tr>
<tr>
<td>CCP</td>
<td>Certified Computer Programmer</td>
</tr>
<tr>
<td>CDP</td>
<td>Certified Data Processor</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>Compact Disk ROM</td>
</tr>
<tr>
<td>CGSB</td>
<td>Canadian Government Standards Board</td>
</tr>
<tr>
<td>CIA</td>
<td>Certified Internal Auditor</td>
</tr>
<tr>
<td>CICA</td>
<td>Canadian Institute of Certified Accountants</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CISA</td>
<td>Certified Information Systems Auditor</td>
</tr>
<tr>
<td>CMA</td>
<td>Certified Management Accountant</td>
</tr>
<tr>
<td>CPA</td>
<td>Canadian Payments Association</td>
</tr>
<tr>
<td>CPA</td>
<td>Certified Public Accountant</td>
</tr>
<tr>
<td>CPM</td>
<td>Critical Path Method</td>
</tr>
<tr>
<td>CSA</td>
<td>Canadian Standards Association</td>
</tr>
<tr>
<td>CSM</td>
<td>Cryptographic Service Message</td>
</tr>
<tr>
<td>CSP</td>
<td>Certified Systems Professional</td>
</tr>
<tr>
<td>DA</td>
<td>Data Administration</td>
</tr>
<tr>
<td>DBA</td>
<td>Data Base Administrator</td>
</tr>
<tr>
<td>DBMS</td>
<td>Data Base Management System</td>
</tr>
<tr>
<td>DEA</td>
<td>Data Encryption Algorithm</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DISH</td>
<td>Data Interchange for Shipping</td>
</tr>
<tr>
<td>DP</td>
<td>Data Processing</td>
</tr>
<tr>
<td>DRP</td>
<td>Disaster Recovery Planning</td>
</tr>
<tr>
<td>EAM</td>
<td>Embedded Audit Module</td>
</tr>
<tr>
<td>EBCDIC</td>
<td>Extended Binary Coded Decimal Interchange Code</td>
</tr>
<tr>
<td>EC</td>
<td>Electronic Commerce</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ECE</td>
<td>Economic Commission for Europe</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>EDICCC</td>
<td>EDI Council of Canada</td>
</tr>
<tr>
<td>EDIFACT</td>
<td>EDI For Administration Commerce and Transport</td>
</tr>
<tr>
<td>EDP</td>
<td>Electronic Data Processing</td>
</tr>
<tr>
<td>EDPAA</td>
<td>EDP Auditors Association</td>
</tr>
<tr>
<td>EEC</td>
<td>European Economic Community</td>
</tr>
<tr>
<td>EFT</td>
<td>Electronic Funds Transfer</td>
</tr>
<tr>
<td>EIS</td>
<td>Executive Information Systems</td>
</tr>
<tr>
<td>ES</td>
<td>Expert System</td>
</tr>
<tr>
<td>ESM</td>
<td>Electronic Security Module</td>
</tr>
<tr>
<td>EUC</td>
<td>End User Computing</td>
</tr>
<tr>
<td>FA</td>
<td>Functional Acknowledgement</td>
</tr>
<tr>
<td>FI</td>
<td>Financial Institution</td>
</tr>
<tr>
<td>FASB</td>
<td>Financial Accounting Standards Board</td>
</tr>
<tr>
<td>FEDI</td>
<td>Financial EDI</td>
</tr>
<tr>
<td>FIS</td>
<td>Financial Information Systems</td>
</tr>
<tr>
<td>FITP</td>
<td>Facilitation of International Trade Procedures</td>
</tr>
<tr>
<td>FOB</td>
<td>Freight on Board</td>
</tr>
<tr>
<td>GAAP</td>
<td>Generally Accepted Accounting Principles</td>
</tr>
<tr>
<td>GAAS</td>
<td>Generally Accepted Auditing Standards</td>
</tr>
<tr>
<td>GAO</td>
<td>General Accounting Office</td>
</tr>
<tr>
<td>GEDIS</td>
<td>Generic EDI Standards Committee</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>IAD</td>
<td>Internal Audit Department</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>IC</td>
<td>Information Center</td>
</tr>
<tr>
<td>ICCP</td>
<td>Institute for the Certification of Computer Professionals</td>
</tr>
<tr>
<td>ICS</td>
<td>Internal Control System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrical Committee</td>
</tr>
<tr>
<td>IIA</td>
<td>Institute of Internal Auditors</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISA</td>
<td>Information Systems Auditor</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>ISP</td>
<td>Information Systems Professional</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITA</td>
<td>Income Tax Act</td>
</tr>
<tr>
<td>ITF</td>
<td>Integrated Test Facility</td>
</tr>
<tr>
<td>JEDI</td>
<td>Joint EDI</td>
</tr>
<tr>
<td>JIT</td>
<td>Just-in-Time</td>
</tr>
<tr>
<td>JT1</td>
<td>Joint Technical Committee-1</td>
</tr>
<tr>
<td>JTC/EDI</td>
<td>Joint Technical Committee on EDI</td>
</tr>
<tr>
<td>KEK</td>
<td>Key Exchange Key</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LSI</td>
<td>Large Scale Integration</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>MICR</td>
<td>Magnetic Ink Character Recognition</td>
</tr>
<tr>
<td>MIPS</td>
<td>Millions of Instructions Per Second</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information Systems</td>
</tr>
<tr>
<td>MRP</td>
<td>Manufacturing Resource Planning</td>
</tr>
<tr>
<td>NACHA</td>
<td>National Automated Clearing House Association</td>
</tr>
<tr>
<td>NWDA</td>
<td>National Wholesale Druggists Association</td>
</tr>
<tr>
<td>OA</td>
<td>Office Automation</td>
</tr>
<tr>
<td>OCR</td>
<td>Optical Character Recognition</td>
</tr>
<tr>
<td>ODETTE</td>
<td>Organization for Data Exchange Through Tele-Transmission in Europe</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OOP</td>
<td>Object Oriented Programming</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSC</td>
<td>Ontario Securities Commission</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>OSF</td>
<td>Open Software Foundation</td>
</tr>
<tr>
<td>PAEB</td>
<td>Pan American EDIFACT Board</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PERT</td>
<td>Program Evaluation and Review Technique</td>
</tr>
<tr>
<td>POS</td>
<td>Point Of Sale</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>QC</td>
<td>Quality Control</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RFP</td>
<td>Request For Proposal</td>
</tr>
<tr>
<td>RFQ</td>
<td>Request For Quotation</td>
</tr>
<tr>
<td>ROI</td>
<td>Return On Investment</td>
</tr>
<tr>
<td>ROM</td>
<td>Read Only Memory</td>
</tr>
<tr>
<td>SAS</td>
<td>Statement on Auditing Standards</td>
</tr>
<tr>
<td>SDLC</td>
<td>Systems Development Life Cycle</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>TDCC</td>
<td>Transportation Data Coordination Committee</td>
</tr>
<tr>
<td>TDI</td>
<td>Trade Data Interchange</td>
</tr>
<tr>
<td>TPA</td>
<td>Trading Partner Agreement</td>
</tr>
<tr>
<td>TQM</td>
<td>Total Quality Management</td>
</tr>
<tr>
<td>TSD</td>
<td>Totally Systems Dependent</td>
</tr>
<tr>
<td>TT&amp;C</td>
<td>Trade Terms and Conditions</td>
</tr>
<tr>
<td>UCC</td>
<td>Uniform Commercial Code</td>
</tr>
<tr>
<td>UCS</td>
<td>Uniform Communication Standard</td>
</tr>
<tr>
<td>UN/EDIFACT</td>
<td>United Nations/EDI for Administration Commerce and Transport</td>
</tr>
<tr>
<td>UPC</td>
<td>Universal Product Code</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Source</td>
</tr>
<tr>
<td>VAB</td>
<td>Value Added Bank</td>
</tr>
<tr>
<td>VAN</td>
<td>Value Added Network</td>
</tr>
<tr>
<td>VICS</td>
<td>Voluntary Inter-industry Communications Standard</td>
</tr>
<tr>
<td>VLSI</td>
<td>Very Large Scale Integration</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WINS</td>
<td>Warehouse Industry Network Standards</td>
</tr>
<tr>
<td>WORM</td>
<td>Write Once Read Mostly</td>
</tr>
<tr>
<td>WP4</td>
<td>Working Party Four</td>
</tr>
<tr>
<td>X12</td>
<td>ANSI EDI Standards</td>
</tr>
</tbody>
</table>
About the Authors

Sally Chan, MA, CMA, is the audit manager of Treasury and Investment Banking Systems at Royal Bank. Before assuming her present position Ms. Chan was the audit manager of Corporate Banking Systems, responsible for auditing and reviewing all Royal Bank’s EDI systems. She chaired the first edition of this book, first published by the EDI Council of Canada, Toronto, 1991, the revised edition was published by the Canadian Institute of Chartered Accountants, Toronto 1993. She is coauthor of EDI Security, Control and Audit, Artech House, Norwood, MA, 1993. Ms. Chan is a Certified Management Accountant, and she holds a Bachelor of Arts degree from the University of Hong Kong, and a Masters of Arts degree from the University of British Columbia. Phone: (416) 348-4753, Fax: (416) 348-4810.

Marshall Govindan, MA, CISA, CIA, is a consultant. He has been senior information systems auditor with Canada’s largest diversified financial institution, the Desjardins Confederation in Montreal, which he represented on a task force which developed the control and audit standards for the Canadian Inter-Financial Institution EDI System. He is coauthor of Manifesto on Information-Systems Control and Management, A New World Order, McGraw-Hill Ryerson, Toronto, 1990. He is a graduate of Georgetown University's School of Foreign Service and George Washington University in Washington, D.C. Phone/Fax: (514) 281–7226

John Y. Picard, MBA, CSP, CDP, ISP, President of CanTeck is a career management and systems consultant, a technical systems auditor, and a lecturer. He studied Electronics Engineering in Chicago and he is a graduate of McGill University. He is coauthor of Manifesto on Information Systems Control and Management, A New World Order, McGraw-Hill Ryerson, Toronto, 1990. He chaired the second edition of EDI for Managers and Auditors, the Canadian Institute of Chartered Accountants (CICA), Toronto, 1993. Mr. Picard is a Certified Systems Professional, member of the ICCP, and a member of the Faculty of EDI Education of the EDI Council of Canada. Phone: (514) 352–1513, Fax: (514) 352–4596.

George S. Takach, is a partner in the law firm of McCarthy Tétrault, in Toronto. Mr. Takach practices corporate commercial law with an emphasis on computer, technology, and related matters. He regularly assists parties with the negotiation and drafting of EDI and VAN agreements, and other computer contracts. He is a special lecturer in Computer Law at Osgoode Hall Law School, York University. He is the author of Contracting for Computers (2nd Ed.), published by McGraw-Hill Ryerson, Toronto, 1992. He is also the author of a survey of the legal issues raised by EDI, and (with others) The Software Business. Phone: (416) 601–7662, Fax: (416) 868–1891.

Benjamin Wright, is the author of The Law of Electronic Commerce, a comprehensive book on the legality of EDI, FAX and E-MAIL, published in 1991 by Little, Brown and Company (Boston and Toronto). He is also the author of EDI and American Law: A Practical Guide (Electronic Data Interchange Association: Alexandria, Virginia, USA, 1989), the first North American book on the legality of EDI. Mr. Wright, an independent attorney and a graduate of Georgetown University Law Center, serves as general counsel for the Dallas–Ft. Worth EDI Users Group. His address is 3431½ Granada Avenue, Dallas, Texas 75205–2233, USA. Phone: (214) 526–5254, Fax: (214) 526–0026, E-mail: bwrigh01@reach.com
EDI Control, Management, and Audit Issues

Here are a few comments from some of the authoritative reviewers of the first and second editions.

■ This book deals with one of the most significant developments in the use of computing. EDI will have a major worldwide impact upon the way business transactions are carried out.
  Belden Menkus, EDPACS, June 1992

■ EDI FOR MANAGERS AND AUDITORS is clearly the most comprehensive and detailed treatment of a question every company serious about EDI must address and resolve. Control issues are treated in more detail here than in any other single published work to date.
  Thomas Colberg, Price Waterhouse
  The EDI FORUM, June 1992

■ The rationale supporting a paperless environment is justifiable only in the light of adequate controls, otherwise it is inviting a variety of losses, even disaster. The proposals regarding the need to implement a compliance program to guarantee the adequacy of controls in closely monitored processes will require that managers and auditors become proactive and work together in ways perhaps never done before.
  Michel Beauséjour CA, Partner
  KPMG Peat Marwick Thorne

■ This book is concise, well written, and easy to use. It is a valuable reference and guide to auditing EDI in modern organizations. It is thoroughly referenced and clearly reflects the eighteen months that went into its preparation.
  Charles K. Davis, Ph.D, CPA
  Director of Research, EDPAA–EDPAF
  EDP Auditor Journal, March 1992

■ One of the most common questions asked by managers at our education courses is, “How do we adequately control our EDI environment and satisfy our auditors in the use of EDI?” Until now, little has been available on this subject, either in North America or around the world, but I am convinced that EDI FOR MANAGERS AND AUDITORS should be required reading for the business manager who has the task of managing and understanding the EDI process. As for auditors, this book should be mandatory reading.
  Marshall A. Spence, President
  The EDI Council of Canada

■ I quite liked the succinct writing style used throughout the book, I particularly enjoyed the chapter on security technology. In less than ten pages, the authors summarize the salient features of the most commonly used security techniques. The chapter on internal controls is also very well written and easy to follow with the objectives and techniques for each control issue indicated in point form. One feature I found extremely valuable was the list of references included at the end of each chapter.
  John W. Yu, M.Sc, CDP, CGA
  CGA Magazine, August 1994
The Information Technology Section

IT Section Membership

The AICPA IT Section provides products and services which will allow you to keep pace with changes in technology and increase your competence in information technology. It will also offer advice that will help you provide information technology services in a more professional — and profitable — manner. Annual membership dues are $100. Section benefits include —

- Subscription to the IT Section’s quarterly newsletter, InfoTech Update, with essential information on new developments in the ever-changing world of technology.
- Technology Guides.
- At least four issues of Technology Alert — one-page releases on up-to-the-minute topics.
- Vendor discounts on selected products and publications.
- Discounted registration to the annual Microcomputer Conference.

For more information on IT Section membership, please call Nancy Cohen at (212) 596-6010.
MEMBERSHIP APPLICATION FORM

AICPA INFORMATION TECHNOLOGY
MEMBERSHIP SECTION

Please enroll me as a member in the AICPA Information Technology Membership Section through July 31. I understand that the $100.00* dues fee covers all membership benefits.

☐ Payment enclosed ☐ Bill me

Name ____________________________
Firm ____________________________
Address ____________________________
City __________________ State __________ Zip ___________
Member Number __________________
Business Telephone __________________

Signature ____________________________

*Dues will be prorated quarterly.

This form may be photocopied.