

Electronic Data Interchange (EDI)

Audit Control Guide



Petroleum Industry Data Exchange
A Standards Committee of the American Petroleum Institute

American Petroleum Institute
1220 L Street, Northwest
Washington, DC 20005



Electronic Data Interchange (EDI)

Audit Control Guide

Petroleum Industry
Data Exchange

A Standards Committee
of the
American Petroleum Institute

February 1992

American Petroleum Institute
1220 L Street, Northwest
Washington, DC 20005

CONTENTS

Introduction v

I. EDI Administration 1

II. Trading Partner Agreements 7

III. Value Added Networks 13

IV. Data Transmission Integrity 19

V. Application Controls 24

VI. Backup and Recovery 28

VII. Conclusion 32

Glossary 33

INTRODUCTION

Electronic Data Interchange (EDI) is defined as the computer-to-computer exchange of business information between trading partners in a standardized format. Transactions can be processed much faster with EDI which enables organizations to increase customer satisfaction, reduce costs, and improve their competitive positions.

In an effort to capitalize on these benefits, the petroleum industry, through the API, has made a major commitment to expanded use of this technology. In conjunction with this effort, the API Internal Audit Committee established a task force to examine related control, legal, and audit issues.

SCOPE

This guide is intended as a reference document in the preparation of more definitive guidelines, programs, and procedures for specific users and business risks. Users of the guide should be alert and responsive to the individual needs of their organization.

The guide was written primarily for audit professionals, but it may also benefit information systems, EDI, Controllers, and legal professionals across the industry. It represents the views and experiences of its authors. An effort has been made to be comprehensive; however, it is not possible to anticipate the control needs of every organization. Certain controls may not be enforceable or even useful in a particular environment.

The basic principles of control, such as segregation of duties, documentation, timeliness, completeness, supervision, and review, are as necessary in EDI as in any other business environment. This guide identifies key exposures and security issues which are unique to the implementation of the technology. It does not replace the traditional application audit program. Rather, it emphasizes the types of controls which apply more specifically to an EDI environment.

This guide focuses on the exchange of data rather than funds. As such, controls specific to Electronic Funds Transfer (EFT) have not been included; however, many of the controls outlined herein could be extended to the EFT environment.

RISKS

When EDI is implemented, business processes become increasingly dependent on the security and control of the communications network and application software. The following are just a few of the risks associated with EDI:

- Unauthorized access to transactions could facilitate industrial espionage or major fraud via transaction manipulation.
- Lost, unauthorized, or inaccurate transactions could cause financial losses.
- Misunderstandings between trading partners over the following issues can damage business relationships and cause lost revenue:
 - What transaction format to use
 - Whether or not to send acknowledgments
 - Responsibility for errors, omissions, or communications problems
 - Changes in third-party services or providers
- Lack of knowledge of laws and regulations governing EDI could create legal liability or unrecoverable losses.

GUIDELINES

- I. **EDI Administration** - This section covers the overall management, including topics such as data security policy, organization, and planning. A coordination function is needed to administer the company's EDI program. The coordinator needs to offer leadership both inside and outside the company and is responsible for establishing guidelines, providing technical assistance, providing a review/advisory role for EDI projects, and communicating EDI issues throughout the company.
- II. **Trading Partner Agreements** - This section describes the essential contents of trading partner agreements which provide the basis for understanding responsibilities and obligations of trading partners. A trading partner agreement addresses the standards and methods of data electronically sent and received between two or more parties. The level of detail and specific content found in a trading partner agreement depends on the importance of the underlying transaction. Decisions regarding whether to include or exclude certain provisions should be based on the significance of associated business risks.
- III. **Value Added Networks (VANs)** - A trading partner may elect to use a third-party service provider, such as a VAN, to obtain certain teleprocessing or other services. This section is similar to the trading partner agreement section but emphasizes internal security procedures of third-party suppliers.
- IV. **Data Transmission Integrity** - This section deals with procedures for internal business systems and telecommunications as they apply to EDI. Topics include:

transaction validation, data mapping, data integrity, error detection and communication.

- V. **Application Controls** - This section covers control issues that generally apply to any application which sends or receives information via an EDI transmission. Emphasis has been placed on processing controls for incoming transactions.
- VI. **Backup and Recovery** - This section includes planning measures which ensure the continuity of business transactions and operations if disruption of EDI services and/or operation occurs. It addresses the need for coordinated backup plans for applications, VANs, and trading partners, and includes requirements for data retention on media which substitute for paper documents.

A particular control may be applicable to more than one of the above sections. In this case, the control has been documented in multiple sections to promote clarity and readability of the guide.

SECTION I EDI ADMINISTRATION

INTRODUCTION

An administrative function needs to exist within each company to address issues particular to EDI and to support and manage the implementation of EDI. The type and size of this organization will vary depending on the company's needs. The organization might consist of a coordinating committee (and possibly subcommittees), a project team, or a full-time coordinator.

Regardless of an organization's type and size, a coordination function is needed to administer the company's EDI program. The coordinator is responsible for establishing guidelines, providing technical assistance, providing a review/advisory role for projects, and communicating EDI issues throughout the company.

RISKS

Risks associated with inadequate EDI administration include the following:

- Lack of a company vision for EDI which may result in misunderstanding and lack of management commitment to EDI opportunities.
- Redundant EDI administrative activities.
- Potential duplication of EDI applications and computing resources.
- Inconsistent EDI approaches.

These risks can result in missed business opportunities or additional cost to the organization.

GUIDELINES

A. Leadership

The coordinator should provide leadership for the company's EDI effort both inside and outside the company. Outside influence is particularly important since business groups typically set EDI standards.

1. The coordinator should promote EDI within the company as follows:
 - a. Creates an EDI vision and strategy for the entire company.
 - b. Acts as the focal point for all EDI activity within the company.
 - c. Gains management's commitment to EDI concepts.
 - d. Generates ideas for linking EDI with business strategies.
 - e. Participates in the operating department's technology planning.
 - f. Promotes EDI solutions.
 - g. Educates and raises consciousness about EDI through presentations.
 - h. Conducts EDI seminars for company employees.
2. The coordinator should influence EDI's direction outside the company as follows:
 - a. Actively participates in EDI focal groups and committees.
 - b. Represents the company by participating in standards setting organizations, groups, and/or committees.
 - c. Holds EDI seminars for suppliers and partners.

B. EDI Guidelines

The coordinator should set internal guidelines for the entire company. Guidelines specific to EDI are needed because of complexities brought to the organization by

incorporating the technology into business practices. EDI guidelines may include the following:

1. Defining EDI and related terms.
2. Identifying opportunities to exploit EDI.
3. Giving advice on and examples of trading partner contracts.
4. Setting basic policies for the company's trading partner relationships.
5. Establishing rules for the conversion of data for use in applications.
6. Setting guidelines for data retention/backup procedures.
7. Establishing minimum requirements for disaster recovery.
8. Issuing data security policies and procedures for those applications impacted by EDI.

C. Business Assessments of New EDI Technologies

The coordinator should keep current on changing EDI technologies and provide guidance in technical areas. In this role, the oversight function might include the following:

1. Providing technical assessments of various EDI technologies.
2. Maintaining an awareness of trends in EDI communications technology.
3. Providing technical consultation to project support teams on communications technology capabilities and alternatives.
4. Providing advice and counsel to project support teams by performing evaluations of specific network vendor services.
5. Recommending translation processes available through standard software.
6. Providing technical assessment of proposed changes to all standards used by the company through industry, national, and international conventions.

D. Review/Advisory Role for EDI Projects

The coordinator should provide review/advisory services for projects and will require easy access to all resources important to EDI. In this capacity, the EDI group should perform the following:

1. Coordinate audit coverage of EDI systems before, during, and after implementation.
2. Communicate with trading partners and help establish appropriate ground rules.
3. Review EDI contracts and assist in contract negotiations with trading partners. Obtains appropriate legal counsel when required.
4. Advise project team on changes required to operational procedures, management control procedures, and computer applications in order to implement the electronic delivery and/or receipt of business documents.
5. Monitor progress of all projects.
6. Assist with implementations to reduce the learning curve and to eliminate redundant applications.
7. Help prioritize projects.

E. Coordinate EDI Legal Issues

Electronic Data Interchange alters business procedures by eliminating the need for paper documents and associated handling procedures. Legal risks are especially troublesome because courts have yet to rule on some EDI issues. The technology raises new legal concerns which must be effectively addressed to ensure organizations comply with federal, state, and local laws, reduce potential legal liability, and avoid partner misunderstandings. When using EDI, strong internal control helps businesses avoid possible litigation.

The coordinator should establish guidelines which assist in reducing legal risks. Currently, legal issues are primarily addressed in trading partner agreements which serve as contracts between trading partners. (See Section II on this subject.) The coordinator should also maintain contact with appropriate legal counsel to keep

current on EDI legal issues. Some areas of legal concern which require attention include the following:

1. ***Legal Proof***

A business must be able to prove, after the fact, the details of transactions communicated between trading partners. Traditionally, evidence was made available by retaining paper documents such as purchase orders and invoices. EDI replaces ink and paper. There is currently no legal precedent for/against allowing EDI representations of legal instruments to be used as legal proof to settle a dispute in a court of law. The law only states that information used in court must be reliable. Therefore, strong internal controls need to be in place to ensure reliability in the EDI environment. In the absence of legal precedent it may be prudent to recommend retaining all three EDI mediums: the untranslated transmission, the translation software and its related translation standards, and the translated data.

2. ***Message Authenticity***

Message authenticity in the world of paper documents includes letterheads or other printing on paper showing origin, handwritten signatures, a notary seal, etc. With EDI, controls which establish authenticity can be placed around electronic messages. Some of these controls may be the same as those for paper documents. Other controls specific to electronic medium may include properly protected passwords, message authentication codes, or cryptographic schemes. If a party wishes to hold its trading partner legally accountable for EDI transactions, it should require that internal controls be in place to ensure authenticity and acknowledgements or confirmations are returned for each transmission.

3. ***Reliable Records***

Data brought to court as legal proof is required to be reliable or trustworthy. Strong internal control is the basis for establishing trustworthiness. If electronic records are to be reliable, they must not be manipulated unless stringent audit trails are in effect, and the person who is entrusted with the records must not have conflicting responsibilities. Logs and data kept in original condition can also help establish the reliability of records.

4. Regulations

Various laws and regulations require businesses to keep records of their transactions and implement controls to ensure record integrity and to guard against fraudulent transactions. The Statute of Frauds, Foreign Corrupt Practices Act, state corporation laws, and tax record keeping regulations are examples of laws or regulations which raise questions of compliance in the EDI environment. The coordinator should stay alert to activities in these areas and coordinate or direct appropriate responses to new developments.

SECTION II **TRADING PARTNER AGREEMENTS (TPAs)**

INTRODUCTION

A Trading Partner Agreement is a contract between two or more organizations trading business transactions through EDI. It documents and clarifies the responsibilities and obligations of the parties involved. In addition, the Statute of Frauds and similar laws require that certain contracts be "written" and/or "signed" to be enforceable. A trading partner agreement can attempt to address these requirements. Model agreements are available from the American Bar Association and other sources. These should be considered when drafting company specific agreements between business partners.

Early exchanges of electronic data, such as the swapping of expense information applicable to joint venture properties, commonly were not supported by written agreements. Under EDI trading, where records are transmitted over a network, trading partner agreements are preferred because the trading process is now more complex and more risk is involved.

Trading Partner Agreements are an effective tool for managing risk and provide the basis for a legal commitment between parties. However, not all exchanges may require one. For example, data may be exchanged for informational purposes only. Where contracts are appropriate, the level of detail in the agreement should be commensurate with the importance of the information exchanged and the associated risks.

RISKS

The basic risks of entering into a business transaction with another organization remain primarily the same after EDI processing is introduced. The difference is that generally accepted risk management practices become outdated, and risk exposure becomes more significant under EDI processing. For example:

- Unexpected changes in hardcopy document formats may cause little concern for an order entry clerk, but an unexpected change in the EDI transaction format could cause erroneous transactions or cause all processing to stop completely.
- Transaction approval was previously verified by human review of the document and the approval signature. Computerized routines are now

required to ensure EDI transactions are properly approved. Heavy reliance is placed on these authentication routines when high volumes of transactions are processed without manual intervention.

- Processing delays can potentially impact greater volumes of transactions and can cause greater financial losses and damage to client relationships. Problem resolution techniques, backup and recovery procedures, and communications between trading partners are examples of controls which should receive increased emphasis to offset this added exposure.

GUIDELINES

Generally, the agreement or an appendix to the agreement addresses the following:

A. Basic Clauses and Procedures

1. **Legal Review of Agreement** - Trading partner agreements involve legal, binding obligations between the signing parties. If not previously addressed in other agreements, the TPA should specify exactly when "title transfer" passes from one partner to another. These agreements should be reviewed by the legal department prior to signing the agreement or implementing the activity.
2. **Authority to Amend Agreement** - Many changes to the agreement are operational in nature and do not require the formal review of legal counsel or upper management. Each party designates the positions or individuals authorized to approve minor working amendments to the agreement. The extent of their authorization to approve such minor amendments and the manner in which such amendments are documented (i.e., in writing signed by both parties) should also be noted.
3. **Termination Clause** - Specifies the duration of the agreement and/or the termination procedures. The agreement should also specify whether or not there is an obligation to do business with the other party or to be responsible for the expenses of the other party related to establishing an EDI system.
4. **Liability Limitations** - Defines the responsible party standard of care, nature, and extent of exposure to damage claims.

- a. *Standard of Care* - Specifies the level of care and proficiency to which the partners will be held and the allocation of liability for any loss caused by errors and/or incompetence.
 - b. *Special, Incidental, Exemplary, or Consequential Damages* - Defines the extent of liability of the parties to the agreement for damages arising as a result of unauthorized disclosure of confidential information, a delay in communications, or omissions or errors in the transmission/receipt of a document defined in the agreement.
 - c. *Force Majeure* - Defines the extent of liability to the parties when they are unable to comply with the provisions of the agreement due to reasons beyond their control. This clause should not limit liability for events which could be anticipated or controlled (e.g., hardware downtime, employee errors, etc.) but should limit the time frame for filing suit. The agreement should also specify whether the errors or nonperformance of third party service providers will be deemed to be beyond the control of the trading partners.
5. **Contractual Obligations** - Provision to acknowledge that all transmitted documents represent legally binding and enforceable transactions.
6. **Notification of Problems** - Problems can occur in the transmission, receipt, or acceptance of data. The agreement indicates the following:
- a. Notification procedures.
 - b. Resolution procedures.
 - c. Methods to be used to document transactions.
 - d. Method of delivery for transactions (e.g., phone call, express mail, etc.).
7. **Disaster Recovery Processing** - Outlines the procedures to follow to facilitate communications in the event EDI processing is not functioning due to a disaster. The agreement should include such things as:
- a. Definition of "disaster".
 - b. Methods to be used to document transactions.