EDI Risk Assessment

The goal of risk assessment in an EDI environment is to determine the probability of undesirable events and their associated costs and to install control mechanisms to minimize risk to an acceptable level.

The vulnerability of an EDI system is high because the failure of the system in any of its three stages - initiation, transmission, and destination - will corrupt transactions. Further following risk can occur in an EDI system:

1. Unauthorized Intruder Accessing Information
   In EDI, inter-organizational communication takes place over the network. Public networks used for sending and receiving transactions may be tapped to intercept transactions. Thus, information is susceptible to interception not only at origination and destination nodes, but also during electronic transmission. Access controls designed to defend against unauthorized initiation of transactions include passwords, dial-back mechanisms, user identification, storage lockout, and different levels of access. Control activities to foil interception during transmission include routing messages through a secured medium, encryption, traffic padding, and confidential electronic envelopes.

2. Loss of Data Integrity
   Corruption of data may occur as a result of erroneous input, poor communication lines, deliberate modification, or malfunction of hardware or software. The public networks over which documents are sent among trading partners are generally not protected, and documents can be read or altered by anyone who has access to the network.

   Controls for data integrity ensure that contents of the message have not been altered. These controls include notarization mechanisms, acknowledgment protocols, computerized audit trails, digital signatures, and edit checks.

3. Lack of Transaction Completeness
   The transactions sent over the communication media are sometimes lost during transmission. If an acknowledgment from the receiver is not received within an agreed-upon time period, then the transaction is presumed to be lost and is retransmitted.

   In such circumstances, the transaction may appear twice at the destination. The risk is that the EDI system may not be able to detect missing, mis-sequenced, or duplicated transactions. Batch totals, sequential numbering, acknowledgment control, and one-for-one checking against the control file are among the control mechanisms that can be used to reduce the inherent risks due to lack of transaction completeness.
4. Unavailability of the EDI System

Human actions, logical reasons, and/or environmental factors may cause the EDI system to become unavailable. Employees' unintentional mistakes, such as deletion of data and lack of proper compliance with roles and procedures, generally cause the unavailability of EDI systems; but natural disasters, vandalism, criminal attacks, strikes, or lockouts may also be culprits.

The communication network is an integral part of EDI, which means that viruses and hacking may also occur. In addition, viruses may spread through the transactions and programs traveling among the trading partners. Off-site backup, redundant arrays of integrated disks (RAID), disk mirroring, fault tolerance, and anti-virus packages can be used to minimize the unavailability of an EDI system.

5. Inability to Transmit Transactions

Many EDI systems are unable to transact business with trading partners because data cannot be translated from one format to another. In fact, absence of a structured data format and standardized definitions of data is one of the most probable causes for failure of EDI.

To mitigate the possible negative effects of improper communication standards, North America and Europe have developed communication protocol standards. In the United States and Canada, the American National Standards Institute (ANSI) has developed data transmission protocol standards designated ANSI X.12. In Europe dominant standards are EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport).

6. Lack of Legal Guidance

The conventional commercial laws that typically facilitate commerce by binding and protecting the trading partners have not been customized to accommodate electronic transmissions. EDI partners should, therefore, address business agreements and related legal responsibilities and obligations of their transactions before they start transacting business over the wire. Proper control activities in defining what constitutes a written and a signed document and other terms of agreements should be designed and used as legal guidance between trading partners. These control activities define and ensure the legality of any given transaction in EDI.

Risk Factors and Control Activities

Risk Factors

1. Unauthorized Intruder Accessing Information.
   a. Hacker accessing the system.
   b. Interception during transmission.
   c. Wire tapping.
2. Loss of Data Integrity.
   a. Intruder modifying/fabricating.
   b. Absence of paper audit trail.
   c. Physical signatures are missing.
   d. Errors introduced in the system.
   e. Corruption by authorized personnel.

3. Lack of Transaction Completeness.
   a. Loss of transaction during transmission.
   b. Duplication of transaction due to retransmission.

4. Unavailability of EDI system.
   a. Logical causes, such as virus, trojan horses, programming errors, hardware and software errors.
   b. Natural causes, such as fire, flood, earthquake, power failure, etc.
   c. Sabotage by authorized person.

5. Inability to transmit transactions

6. Lack of legal guidance

Internal Controls

1. Access Control.
   1. Password; dial-back mechanisms; user ID; storage lockout; different levels of access.
   2. Improving cable protection; routing message through secured medium; fiber optics; encryption; traffic padding; confidential electronic envelope. Signal meters; leakage protectors; electromagnetic shielding; penetration resistant conduits.

2. Authentication.

3. Acknowledgment.
   1. Batch totaling; sequential numbering.
   2. One-for-one checking against the control file.

4. Fault tolerant systems.
   1. Anti-virus packages; error free software and hardware.
   2. Off-site backup; RAID; disk mirroring
   3. Training; dissemination of procedure and policies on control.
   4. Structured/standardized data format; adherence to ANSI/EDIFACT protocol.
   5. Agreement on legal definitions, responsibilities, and obligations.