8-25-1995

Association for Information SystemsAmericas Conference on Information SystemsEDI Risks, Security and Control: An Australian Survey

Swee Beng Lim
UNSW, Sydney, NSW

Rodger Jamieson
UNSW, Sydney, NSW, r.jamieson@unsw.edu.au

Association for Information Systems Americas Conference on Information Systems

EDI Risks, Security and Control: An Australian Survey

Swee Beng Lim - Research Student
and
Rodger Jamieson - Senior Lecturer
School of Information Systems, UNSW, Sydney, NSW 2052
Contact: Phone: (61)-2-385-4414, email: r.jamieson@unsw.edu.au

Introduction

Electronic Data Interchange (EDI) is the inter-change of business documents between organisations in a structured, machine-retrievable data format, allowing data to be transferred, without re-keying, from an application in one location to an application in another location (Hansen and Hill, 1989). Security and controls are important in EDI because its widespread use as a business tool has not only changed the way business is conducted, but also introduced potential new risks which need to be addressed. In particular, cross-vulnerabilities which exist between inter-dependent trading partners in an EDI network put companies at risk due to the "domino effect" of one partner's errors or security failures compromising the integrity of other partners' systems (Marcella and Chan, 1993; Chan et al, 1991; ICAEW, 1992). Furthermore, the automation with which transactions are processed at high volume and speed has led to reduced opportunities to spot problems using human intuition (ICAEW, 1992).

To explore organisational attitudes towards EDI risks and the importance of control issues, research was conducted on EDI-using organisations in Australia using a survey and case study approach. The primary aim of the survey is to obtain organisational perceptions on EDI risks, the importance of EDI controls, and the risks and controls considered important in EDI. The case study gives an in-depth perspective on the strategic and management issues considered by a major EDI-using organisation to achieve a successful EDI implementation.

Research Method

As part of the research effort, an extensive literature survey was done in order to develop a normative framework of risks and the corresponding controls for mitigating the risks.

This framework was then used as a theoretical basis for developing concepts and constructs for the survey and case study research.

In order to address the research questions, a mail questionnaire was designed to measure perceptions relating to EDI risks and control issues from technical executives and auditors. Most items were measured using Likert scales and presented in two separate questionnaires, one for technical executives and one for auditors.

The sample for the study consisted of 252 organisations taken from a mailing list kindly furnished by the EDI Council of Australia. One technical executive survey and one auditor survey were sent to each firm. Following the mailing of reminder letters and follow-up phone calls, 40 useable surveys were returned.

Research Findings

Overall Risk and Importance of Controls

While the overall perception by the respondents indicates that the risk in EDI is average in significance, a detailed analysis of the survey data reveals a distinct difference in perceived risk levels between technical executives and auditors. Auditors perceived a 'slightly/high to high' risk in EDI while technical executives perceived a 'slightly/low to average' risk (a between-group T- test was significant at $p < 0.01$). In contrast to auditors, technical executives did not view EDI as a high risk method of message transfer.

Paired T-tests between respondent groups' ratings of overall importance for each control area showed no significant differences, suggesting that both technical executives and auditors regard controls in the areas of EDI implementation, EDI operation and network service to be 'slightly/high to high' in overall importance.

Ranking of Risks and Controls

Two methods of analysis were employed to identify the most significant EDI risks and controls. Kendall's test of concordance and Weighted Votes were used respectively for the Likert-scale responses and the rank votes. Weighted Votes are calculated by assigning the highest (5) through the lowest (1) points consecutively to a first place ranking up to a fifth place ranking, and then summing the points for each factor. Only the top 5 votes cast by each respondent are considered. Kendall's Test of Concordance is a non-parametric test that ranks the factors in order for each case, calculates the mean rank for each factor over all cases, and then calculates the Kendall's W. W ranges between 0 and 1, with 0 signifying no agreement and 1 signifying total agreement. These methods produced a list of preference values used for ranking of factors under each category of risk and control (that is, implementation controls, operational controls and network controls). The ranked factors are obtained for each category and respondent group, and are presented in Tables 1 through 4.

Ranking of EDI Risks

The most significant risks include those associated with (1) loss or delay of documents during transmission, (2) errors or alterations introduced into messages, (3) network inter-connection risks and (4) risks arising from inadequate record retention controls and legal liability.

Table 1: Ranking of risks in EDI by technical executives and auditors

	Technical Executives' Rankings		Auditors' Rankings	
	*Kendall's Test	Weighted Votes	+Kendall's Test	Weighted Votes
Inter-connection risks	1	3	4	10
Non-delivery or delayed delivery	2	1	8	4
Incorrect tables or software	3	4	7	6
Inaccurate, incomplete trans	4	2	2	1
Record retention risks	5	5	5	2
Potential legal liability	6	6	3	3
Difficult to audit	7	7	1	7
Denial of services	8	9	12	12
Disclosure of contents	9	10	10	11
Repudiation of origin/receipt	10	11	9	8
Alteration of computer files or software	10	8	11	9
Non-authentic, unauthorised transactions	11	9	6	5

*W = 0.20, p < 0.001
+W = 0.15, p < 0.001

Ranking of Implementation Controls

The most important implementation controls include (1) top management support, (2) communication with trading partners throughout the implementation phase, (3) explicit treatment of EDI in IT strategic and business plans both short term and long term, and (4) review of existing applications, internal systems and business operations, for example, to determine how these can operate effectively under EDI and what additional controls need to be incorporated.

Table 2: Importance ranking of implementation controls

	Technical Executives' Rankings		Auditors' Rankings	
	*Kendall's Test	Weighted Votes	+Kendall's Test	Weighted Votes
Top management support	1	1	2	1
Communication with partners	2	3	1	7
Treatment of EDI in strategic plans	3	2	3	2
Review of existing operations	4	4	4	3
Establishment of task force	5	6	7	6
Training and education	6	5	9	3
Quality project plan	7	10	8	12
Formal development methodology	8	8	10	5
Participation in industry group	9	7	16	10
Cost and benefit analysis	10	9	12	3
Evaluation of vendor software	11	11	11	11
Network service agreements	12	12	13	9
Evaluation of network provider	13	13	14	13
Trading partner agreements	14	11	5	8
Security and risk analysis	15	9	6	4
Audit involvement	16	14	15	10

*W = 0.33, p < 0.001
+W = 0.12, p < 0.001

Ranking of Operational Controls

Table 3: Importance ranking of operational controls

	Technical Executives' Rankings		Auditors' Rankings	
	Kendall's Test	Weighted Votes	+Kendall's Test	Weighted Votes
Follow-up procedures for errors	1	6	2	5
Contingency planning and backup	2	4	3	3
Software upgrade procedures	3	5	10	7
Record retention practices	4	11	7	9
Access controls on files/programs	5	2	8	11
Application controls in software	6	1	1	1
Reports for tracking transactions	7	7	6	5
Acknowledgements	8	3	9	4
Change controls on software and tables	9	8	5	6
Sequence numbers in messages	10	5	4	2
Written policies and procedures	11	15	13	12
Audit and management trails	12	10	12	10
Matching trans with records	13	9	14	8
Accounting controls	14	12	11	6
Encryption mechanisms	15	14	17	14
Manual checks	16	13	16	13
Segregation of duties	17	10	15	14

*W = 0.31, p < 0.001
+W = 0.30, p < 0.001

The most important operational controls include (1) procedures for following-up of transmission errors or suspense items, (2) contingency planning and backup, (3) application controls in software to provide, for example, edit checks, control totals check or matching against trading partner profiles, (4) the use of acknowledgements to track transactions, and (5) the use of sequence numbers by software to detect duplicate or lost transactions.

Ranking of Network Controls

Table 4: Importance ranking of network controls

	Technical Executives' Rankings		Auditors' Rankings	
	*Kendall's Test	Weighted Votes	+Kendall's Test	Weighted Votes
Comms. protocols for error recovery	1	1	2	1
Procedures for delivery failures	2	2	1	3
Fall-back measures for network failures	3	3	6	9
Restrict access to data/logs	4	8	3	4
Safeguards over network access	5	5	4	2
Audit trails of network access	6	10	5	7
Retention of transaction logs	7	7	8	6
Network/mailbox reports	8	4	9	8
Capability of network support staff	9	6	12	12
Screen new partners for mailbox	10	11	10	10
Authorisation mechanisms	11	9	7	5
Central approval for mailbox changes	12	12	11	12
Security reviews on network systems	13	13	13	11

*W = 0.18, p < 0.001
+W = 0.27, p < 0.001

The network controls voted as most important include: (1) communication protocols for error recovery, (2) procedures for notifying failures in message delivery, (3) safeguards over network access control, and (4) measures to restrict access of network organisation staff and outsiders to data in mailboxes or transaction logs.

Determinants of Overall Risk and Importance of Controls

A minor aim of the research was to study the effect of organisation and system context variables on the overall perceptions of risk and the importance of EDI controls. The most significant determinants which tend to change the level of these perceptions are the degree of EDI integration with applications, transaction volume, transaction value and the transaction type.

The Case Study

The case study identified the strategic and management factors contributing to the successful implementation of EDI within a major EDI-user organisation. These factors include (1) a strategic treatment of EDI in business and IS plans, (2) commitment from key senior managers, (3) relationship building with major customers, (4) effective marketing strategy to sell EDI to suppliers, (5) keeping abreast with national and international developments through participation in industry working groups, and (6) audit involvement. Findings from the case study attest to the survey results in regards to the management factors essential to the successful implementation of EDI.

Conclusion

This research has demonstrated that results of this survey are congruent with survey results previously reported and, this therefore gives a fair amount of confidence with respect to its reliability. However, the overall reliability of the survey needs to be assessed in the light of the relatively low response rate and the fact that the majority of the responding organisations were small to medium users of EDI. The results are therefore more representative of this particular class of EDI users and should not be used as a generalisation for the whole population. Nevertheless, this research has provided an exploratory framework which can be used as the basis for developing concepts, constructs, and methods for more detailed, systematic descriptive or explanatory studies.

Bibliography

Chan, S., Govindan, M., Picard, J.Y., Takach, G.S. and Wright, B. EDI for Managers and Auditors, The EDI Study Group, EDI Council of Canada, Toronto, Canada, 1991.

EDICA, EDI Control Guide: Make your business more competitive, EDI Council of Australia and the EDP Auditors Association, 1990.

EDICA, EDI Message Security Guide: Protect your business communications, EDI Council of Australia, 1991.

Hansen, J.V. and Hill, N.C. "Control and Audit of Electronic Data Interchange", MIS Quarterly, December 1989, pp. 403-413.

ICAEW, Institute of Chartered Accountants in England and Wales - EDI Working Party, "Harnessing EDI, Controlling the Business Risks", Institute of Chartered Accountants in England and Wales, U.K., 1992, pp. 1-43.

Jamieson, R. EDI: An Audit Approach, EDP Auditors Foundation, Inc, Research Monograph Series No.7, April 1994, pp. 1-93.

Marcella, Jr. A.J. and Chan, S. EDI Security, Control, and Audit, Artech House, 1993.