EDI
Audit and Control

Edited by

Ian Walden

and

Ashley Braganza

EDI: Audit and Control

I. Walden

A. Braganza

NCC Blackwell
MANCHESTER • OXFORD

British Library Cataloguing in Publication Data.

EDI: Audit and Control.
I Walden, Ian II. Braganza, Ashley.
384.3

ISBN: 1-85554-208-0

1. Electronic data interchange
2 Auditing – Data processing.

First published in 1993 by:

NCC Blackwell Ltd, 108 Cowley Road, Oxford OX4 1JF, England.

Editorial Office: The National Computing Centre Limited, Oxford House, Oxford Road, Manchester M1 7ED, England.

Typeset in 10/12 Times by Icon Graphic Services, Exeter.
Printed in Great Britain by T.J. Press (Padstow) Ltd, Padstow, Cornwall.

Preface

Electronic Data Interchange is the exchange of structured data. Such exchange can occur between a whole range of communicating entities, including trading partners and with regulatory authorities. Over the past few years, the growth in the use of EDI has progressed rapidly into an ever greater variety of areas, from payments to education. However, the effective long term exploitation of EDI communication techniques, as *the* communication medium to replace paper, depends on one key aspect: Do the communicating entities have confidence and trust in the systems and procedures involved, and can they establish such confidence in the minds of their trading partners? Without confidence, such systems will not provide the real efficiency benefits that EDI promises. Establishing trust depends on our ability to control the operation of EDI, and the central theme of this book is how to establish such control.

Control, as defined within the context of this book, has three complementary components: Technical security, audit and legal. This book considers how these elements need to be given adequate consideration during the implementation of EDI systems to ensure that such systems operate successfully, and therefore maximise the benefits that accrue from the investment in time and resources.

The purpose of this book is to give clear guidance to EDI managers, practitioners and their professional advisors in the complex issues raised by the introduction of paperless trading. The chapters in the book attempt to give the widest possible consideration to the EDI audit and control issues. Where necessary, in the readers' interest, fuller explanation has been sacrificed for clarity:

- **EDI development** reviews the current state of EDI use within Europe and identifies some future areas into which EDI is likely to spread.

- **Records management** considers the need for organisations to establish procedures to control the creation, distribution, storage and destruction of the whole range of communications and documents that an organisation deals with on a day-to-day basis, and how EDI record keeping fits within this general task.

- **The impact of EDI on audit** is divided into three separate sections. The first reviews the nature of the audit and accounting function and the extent to which the traditional financial audit needs to take account of EDI usage. The second considers the role of audit in assessing the effectiveness of EDI security procedures. Finally the potential for auditing the performance of an EDI network provider is analysed.

- **EDI and public sector auditing** is in two sections. HM Customs and Excise are enthusiastic proponents of EDI, although they need to ensure that the system functions correctly in order that organisations can fulfil their statutory obligations, eg. self-billing systems. This section details the scope of such requirements and the position taken by the Authority. The Health Service is a classic public sector example of how EDI can reap significant benefits in terms of efficiency, and the second section provides a case study of how the audit and control implications have been tackled in this public sector environment.

- **EDIFICAS** is the European interest group in the area of accountancy. This chapter reviews progress in the development of EDI messages that can be adopted for the communication of accounting data. It discusses the nature of the traditional data used within the accounting process and the extent to which it can be reinterpreted in an EDI context.

- **Risk analysis** is the key first step in recognising the nature of the risks that arise when implementing EDI, therefore enabling an organisation to construct a policy framework aimed at counteracting such vulnerabilities.

- **Technical security** reviews the nature of the security techniques required to fulfil the key elements of data security: confidentiality, integrity and availability. In particular, the nature and role of encryption techniques is described in a clear and accessible fashion for both commercial and technical managers.

- **ITSEC** is a government sponsored scheme designed to enable companies to have their IT products and services certified as achieving a certain degree of ‘assurance’. The chapter describes the nature of the scheme, and the role it could play in securing EDI systems.

- **Record-keeping and evidential requirements** examines the reasons why organisations need to maintain EDI records within Europe. The US chapter considers the extent to which an ‘internal record keeper’ could act as guarantor of secure EDI.

- **Establishing legal security** discusses the legal consequences of implementing EDI. The two major EDI agreements, with the message recipient and the EDI network provider, are considered on a clause-by-clause basis in the context of establishing legal security.

- **Auditing EDI** includes two practical case studies of how EDI audit and control issues have been dealt with, in both the private and public sectors.

We, the editors, hope that the book serves as an important reference tool for those commencing on the process of EDI implementation, as well as existing users, who need to ensure that all necessary audit and control issues have been given adequate consideration.

Ian Walden
Ashley Braganza

January 1993

Biographies

• Editors

Dr Ian Walden has done research, consultancy and lectured in a wide variety of subjects relating to computer law. He has written numerous texts in the field and is editor of EDI and the Law (NCC Blackwell 1989) and joint editor of Information Technology & the Law (2nd ed., Macmillan 1990). Ian a member of the editorial team for the journal Computer Law and Practice. Ian is a member of the UK EDI Association's Legal Advisory Group, and the ICC (UK) Computing, Telecommunications and Information Policy Committee. Ian is currently the Tarlo Lyons Information Technology Law Research Fellow at the Centre for Commercial Law Studies, Queen Mary & Westfield College (London University) and is a consultant to London solicitors, Tarlo Lyons

Ashley Braganza joined the Information Systems Group in the Cranfield School of Management in May 1991. He has been working on a two year research project, 'EDI: The longer term effects upon business'. His key areas of responsibility are the financial and commercial aspects of EDI. Ashley has also worked for the European Commission, TEDIS II Project B.11 'EDI and financial operations'.

In addition to these projects, Ashley lectures to the full-time and executive MBA's on Information Management. Ashley is currently working towards a doctorate in the area of strategies and key success factors for busines process redesign.

Prior to joining Cranfield, Ashley was the Strategy Manager in Midland Bank's EDI services department. He has also completed an MBA at the Strathclyde Business School.

• Contributors

David G.W. Birch graduated from the University of Southampton with a B.Sc (Hons.) in Physics and then joined Logica, where he spent several years working as a consultant specialising in communications. In 1986, he was one of the founders of Hyperion and now provides specialist consultancy to a variety of clients. He has lived and worked on a wide range of information systems in the U.K., Europe, the Far East and North America for clients as diverse as SWIFT, the London Stock Exchange, the Ministry of Defence and the Indonesian PTT. He is a

Visiting MBA Lecturer in Information Technology Management at the City University Business School in London, Chairman of the IISyG Working Group on Information Security & Society and the author of a number of papers on the subjects of security and risk.

The author can be contacted at Hyperion, 8 Frederick Sanger Road, Surrey Research Park, Guildford, Surrey GU2 5YD, United Kingdom.

Christophe Brunet is EDI Deputy Manager at GSI Telematique, and is specialised in service quality and service level agreement issues for EDI.

Joanne Curson. Computer Auditor, Norwich Systems and Accounting. Joanne qualified with the Institute of Chartered Accountants in 1991, having spent a good deal of her training working as a computer auditor in the private sector. She is now looking to build on her experience to date by playing a lead role in the delivery of computer audit services to various Health Authorities and hospitals throughout East Anglia.

Sandra Davies is the EDI Manager at Asda Stores and is responsible for the development and implementation of EDI with Asda's trading partners. She manages an EDI unit which provides implementation, support and training for Asda and its suppliers.

After joining the company in 1989 as a Store Administration manager, she became a Regional Administration Manager responsible for the administration, training and the implementation of store finance systems.

Sandra is a member of the Institute of Training and Development. She has been invited to speak at conferences and workshops on the managerial aspects of EDI.

Malcolm Gorringe. Director of Audit & Consultancy Services, Norwich Systems and Accounting. Malcolm has spent virtually all his time in internal audit and consultancy since qualifying in 1977 with the Chartered Institute of Public Finance & Accountancy. His experience to date has covered both `fieldwork' and various junior, middle and senior management positions with Local Authorities and the National Health Service. He has always been at the forefront of developments in auditing and auditing techniques at local, regional and national level. He has written articles, given presentations and chaired a number of reginal groups and seminars. Recently, Malcolm has provided help and support to a number of Internal Audit Departments seeking to respond effectively to the challenges and opportunities flowing from the NHS reforms.

Richard Griffiths has nine years experience developing information systems, most recently with Logica and Midland Bank. He played key roles in the development of Midland's TradePay EDI service, and the Dutch PTT's X.400-based Sagitta and Tradeserver EDI systems.

Pascal Grin graduated from the Ecole Supérieure de Commerce de Paris as a Chartered Accountant. He joined Ernst & Whinney (now Ernst & Young) in 1979 as an external auditor, which he left in 1983 as an Audit Senior.

From 1983-84 he was a Controller with Johnson & Johnson, and then occupied several functions within the Thomson Group, all of them in connection with the accounting function. He left Thomson as Director of International Accounting within SGS-Thomsen Microelectronics.

He joined Schering in 1990, and has recently been appointed Director of Finance and Adminstration within Schering S.A. (France).

Matthew Heim, born in the United States of America and educated at the Universities of Maryland and Southern California, has spent the past 14 years living in Europe. During this period of time, Mr Heim has been working as a consultant in the field of information technology, designing and implementing systems for many major enterprises and authorities throughout Europe, including the European Commission, the German Railroad and the US Department of Defence. Mr Heim is currently employed with KPMG in Frankfurt, Germany, consulting and performing audits in the areas of electronic data interchange and distributed systems.

William List CA FBCS is a director of The Kingswell Partnership, a consultancy which specialises in assisting organisations to limit business risks in the use of IT.

He spent 25 of his 30 years service with a major accounting and consulting firm specialising in the creation of procedures to prevent or detect errors and fraud in computer processing. He is an acknowledged expert in the use of control and security techniques in application systems, including those involving networks, EDI and distributed processing. He has made a study of the accounting, security and control issues in EDI systems and led the team in KPMG who produced a booklet for the EC under the TEDIS programme entitled "Secure EDI - a management overview."

He has spoken at many international conferences on EDI, accounting, auditing, security and control topics. He is Secretary of the BCS Security Committee and Chairman of IFIP working group 11.5 - System integrity and control.

Stephen Marsh is a Principal Consultant with Secure Information Systems Limited (SISL), a specialist UK consultancy and systems integrator who operate one of the original Commercial Licensed Evaluation Facilities (CLEFS). Stephen specialises in the audit, design and evaluation of secure IT systems, and in research and development of practical solutions to stringent security requirements. Prior to joining SISL, Stephen was a consultant with SD-Scicon and a software engineer with Logica.

Robin Nicholson has 28 years professional experience in Information Systems largely gained in the commercial sector where he has worked for users, manufacturers, systems houses and consultants. During this time he has progressed through most roles from programming and analysis to project management and direction.

His present role is Head of the Information Systems Division of the Dental Practice Board where he manages a large mixed technology computing environment. In this role he plays a major part in satisfying one the DPB's corporate objectives: progressing the organisation toward a low cost technology intensive operation with minimum clerical intervention.

Robert Picard has worked as a network and information system specialist at

France Telecom. He joined the Ministery of Post and Telecommunications, where he was in charge of the regulation for value added networks. He works now for GSI, as Head of the Strategy and Marketing for the Telematique division, in charge of the EDI service.

Graham Robson, a graduate of Lancaster University, worked for several years in business development for Griffin Factors, a part of the Midland Bank Group.

He moved to Asda Stores in 1986. Since that time he has filled a number of management roles in the finance department, latterly as Financial Services Controller. This role includes implementation of EDI within Asda.

Ken Slater is a Managing Consultant with Touche Ross, specialising in computer and network security. He has 30 years experience in computing and 15 years in computer audit and security consultancy. His consultancy activities have included reviews and implementation of security measures in a wide range of organisations in the public and private sectors, including large mainframe installations, national and international networks and multi-customer bureaux. He is currently the UK National Security office for Touche Ross and he lectures and writes extensively on security matters. His latest book "Information Security in Financial Services" was published in November 1991.

Graham Southwood is currently Chairman of the Records Management Society and for five years was editor of the Records Management Bulletin. He became interested in records management when he was given responsibility for advising on registry systems whilst on secondment to the Cabinet Office. This led him to developing a records management programme aimed at influencing records managers in the Civil Service as a whole. He is currently senior business consultant at Business Data Management, one of the largest data storage companies in the UK.

David Watt is an audit manager with the Headquarters Computer Audit Unit of HM Customs and Excise.

Having spent his early career on VAT control, he specialised in 1981 in computer systems audit. He has been heavily involved in EDI since 1983 and now represents HM Customs in addressing VAT issues associated with electronic invoicing. He also acts as an external advisor to a number of EDI Standards bodies and trade/industry associations in meeting the Revenue control needs of emerging EDI initiatives.

Bernard Williams graduated with an engineering degree from Imperial College, London, a doctorate in accounting from the University of East Anglia, Norwich and is a qualified chartered accountant. Currently he is the head of accounting and finance in the School of Information Systems at the University of East Anglia and ICAEW Research Fellow. Dr Williams is the UK representative on the accounting message development group of EDIFICAS Europe, a member of the IT advisory committee of the Chartered Association of Certified Accountants, and the author of three books and various articles on different aspects of IT and accounting.

Benjamin Wright, a Dallas, Texas-based attorney, is the author of The Law of Electronic Commerce: EDI, Fax and E-mail, a treatise published with annual supplements by Little, Brown and Company, Boston, Toronto and London. Wright invites comments on the ideas expressed here. His address is 3431-1/2 Granada, Dallas, TX 75205, USA, Tel: 214-526-5254, Fax: 214-526-0026.

Contents

1

EDI Developments around Europe

Ashley Braganza

1.1 Introduction

The purpose of this chapter is to provide the reader with an overview of EDI developments around Europe. There are quite remarkable differences between the various countries. These differences range from the take up of EDI to standards being used and the state of the telecommunications industry in the country.

Within this chapter EDI is defined as the electronic transfer of information from one organisation's application to another organisation's application using standards.

1.2 EDI Users

1.2.1 The level of EDI usage

The number of users varies significantly across Europe. In the UK there are about 6000 EDI users. This ranges across all industries, retail, construction, transport and logistics, manufacturing and financial services.

Other European countries which have large EDI communities include France, Germany, and Italy. EDI users can be found in other countries such as Spain, Belgium, Netherlands and Ireland but these communities tend to be focused around specific industries. For example, in Spain the automotive industry has the largest user base.

There are trials and pilots being actively developed in almost all major industries in each European country. In Switzerland, for example, trials are currently underway in the distribution sector with customs taking an active role.

In other countries, Greece and Portugal for instance, EDI is not used at all at the current time.

1.2.2 The spread of EDI

The development of EDI has also varied significantly (see also Section 9.9.4). To understand this one needs to hold in one's mind the image of a supply chain. In a typical supply chain there are up-stream activities in which raw material manufacturers sell to value added manufacturers, who sell to distributors; and down-stream activities in which distributors sell to retailers, who sell to consumers.

In several countries such as Denmark, France and UK the push for EDI has come from the down-stream end of the supply chain. The types of messages include retailers sending orders and receiving invoices from distributors and manufacturers.

One of the key forces for implementing EDI at this end of the supply chain is the sheer volume of messages which flow between organisations. In addition to orders and invoices, the following are only a few of the documents which also get exchanged: price and discount files, delivery notes, proof of delivery notes, returned goods notes, and credit notes.

EDI has started to be used by some of the up-stream organisations in the supply chain. However, often there are insufficient volumes on which to justify the use of EDI. For example, in the case of organisations which supply their products in bulk, such as chemicals or flour, then very typically there are long term contracts in place between the raw material manufacturer and the value added manufacturer. The volume of messages which could be sent using EDI is extremely low because the value added manufacturer would tend to place perhaps, one order a week.

1.2.3 Financial EDI (FEDI)

While organisations have started using logistics EDI in most areas, FEDI has had an extremely slow start. In some countries, such as the UK, the banks have set up FEDI services (see Future Developments below) but the take up of the services has been extremely limited. The banks in other European countries plan to provide FEDI services; however, few banks have developed FEDI services. The banks in Netherlands are not unlike the banks in many of the other European countries: the major banks are involved in FEDI pilots and plan to use the pilots as a basis on which to provide FEDI services in the future.

The need for a strong audit and control procedure becomes more necessary as FEDI services become available. In the UK, where FEDI services are arguably the most highly developed, security is a major concern to corporates. FEDI can be done with much greater speed and transparency, and without the levels of manual intervention often associated with traditional payment methods. This means that corporates need to have in place clear audit trails and control procedures which ensure their EDI payments systems do not get misused.

Whereas a similar statement could be made about logistics EDI: clear audit trail and control procedures, the misuse of the EDI payments system is likely to have a far greater impact on the organisation than misuse of order and delivery notes, for example.

1.2.4 Public Sector

Another key user in the EDI arena is the public sector (government). In several European countries, parts of the public sector have been extremely active in using EDI, as well as setting out rules for corporate usage, funding pilots and partaking in EDI groups and associations. In the UK, Her Majesty Customs and Excise have been instrumental in enabling corporates to set up, for example, invoicing systems and audit procedures (Section 4.2). Other government departments and agencies such as Education and HM Stationery Office are either currently using EDI or plan to use EDI in the near future.

In several countries such as Switzerland, Ireland, France and Italy, departments like customs and port authorities are moving the usage of EDI forward. An interesting development is that local governments in many European countries have started showing an interest in using EDI for exchanging information with central government. This will further focus the minds of managers who are not yet convinced about whether EDI is here to stay.

1.2.5 Small and Medium Enterprises (SME)

One major issue for the larger EDI users is while they often have the economies of scale which enable them to recoup their EDI investments, SMEs are rarely able to do so. This has meant that few, if any, EDI communities in any European countries have a strong SME representation. SMEs implementing EDI usually do so because they are suppliers to corporates which have a stronger position than them.

1.2.6 EDI and the Telecommunications Networks

One issue which should be mentioned, albeit briefly, because it affects the take up of EDI quite fundamentally, is the quality of the national telecommunications network. In countries where there exists a well functioning telecommunications network, the take up of EDI has been high. And even if the initial take up has not been high, industries and organisations, within the country, have been able to start pilots and trials on which future EDI usage will be based.

However, where the provision of telecommunication services is poor not only does EDI not exist but it is also difficult to see organisations using EDI until the situation is reversed in some way. It could be argued that these countries could take advantage of newer technology such as satellite communications. However, the timescales for putting an infrastructure in place may put the country at a disadvantage if other trading partner countries move too far ahead. In a European context this could be a major issue for EDI usage in the 1990s.