INFORMATION SYSTEMS AUDITING AND ELECTRONIC COMMERCE

By

HAROLD J. WAGNER, CISA

A MASTER'S PROJECT

Submitted in partial fulfillment of the requirements for the degree of
Master of Science in Management Information Systems

COLLEGE OF BUSINESS AND MANAGEMENT
UNIVERSITY OF ILLINOIS AT SPRINGFIELD
SPRINGFIELD, ILLINOIS

FALL 2001

jwagner74@juno.com

jwagner74@juno.com

GRADUATE PROJECT/~~THESIS~~ ACCEPTANCE PAGE

Submitted by Harold Wagner in partial fulfillment of the requirements for the degree of Master of Science in Management Information Systems.

Accepted on behalf of the Faculty of the College of Business and Management by the project/~~thesis~~ committee:

Rassule Hadidi
Project/~~Thesis~~ Supervisor

James Hall
Student's Choice

John Nosari
Dean's Choice

Rassule Hadidi
Department Chairperson

12-20-01
Date of Committee Approval

Paul McDevitt, Interim Dean
College of Business and Management

1/22/02
Date of Dean's Approval

TABLE OF CONTENTS

jwagner74@juno.com

jwagner74@juno.com

LIST OF ILLUSTRATIONS

jwagner74@juno.com

ABSTRACT

Information Technology has become a vital resource to almost every person in the world, whether they know it or not. With approximately 500 million people connected to the Internet (http://www.nua.ie), along with the growth of technology, Electronic Commerce is being considered by entities of all types, be it an individual or an organization. Electronic Commerce involves using Information Technology to transmit data, which is often sensitive, over the Internet. The use of the Internet to transmit sensitive data makes the data increasingly vulnerable, and subject to undesirable consequences resulting from deficient control. Reducing this potential is the challenge of Information Systems Auditing.

While there is an abundance of data on both Electronic Commerce and Information Systems Auditing, information pertaining to an interrelationship between the two subjects has been limited. Therefore, the result of this project was threefold. First, the project identified common and significant deficiencies in e-Commerce. Second, it involved determining control requirements not adequately addressed by existing methodologies and frameworks. The end result of this project is a compilation of control practices that address issues not addressed by existing methodologies: a "bridge" between the "what is" and the "what should be."

jwagner74@juno.com

CHAPTER ONE – INTRODUCTION

Information Technology is finding its way into almost every aspect of the world. Many people depend on Information Systems for some aspects of their day-to-day lives. Even those who do not know what an Information System is depend on it indirectly for common necessities, such as utilities, insurance, and medical treatment. In addition, virtually every organization is considering Electronic Commerce in some form. Electronic Commerce (e-Commerce) has the potential to dramatically change the way the entire world does business; and I am certain it will. With these advancements, particularly with the increased user base (including customers) and an increasingly widespread transmission of sensitive data, also arise an increased potential for undesirable consequences resulting from deficient control. Reducing this potential is the challenge of Information System Auditing.

On May 18, 1998, I began employment as an Information System Auditor, and on September 17, 2001 I was awarded the Certified Information Systems (IS) Auditor (CISA) designation by the Information Systems Audit and Control Association (ISACA). On October 1, 2001, I was promoted to an IS Audit Supervisor. Throughout my employment, I have received training and continuing education courses related to IS auditing. I have incorporated various frameworks and methodologies used by my employer, such as Control Objectives for Information and Related Technology (CobiT), System Auditability and Control (SAC), Audit Control Evaluation System (ACES), Federal Information Systems Control and Audit Manual (FISCAM), and Federal

Information Processing Standards (FIPS). Additionally, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has been a valuable source of audit and control information (http://www.coso.org).

STATEMENT OF THE PROBLEM

Information Systems Auditing is not limited to finding weaknesses and recommending ways to strengthen a system. It must also include substantiating such findings, and most importantly, adding benefit to the organization. Adding to the complexity of this significant challenge is an incredibly fast rate of technological change, and the lack of historical precedent. This is especially true with Electronic Commerce, where there is limited control guidance.

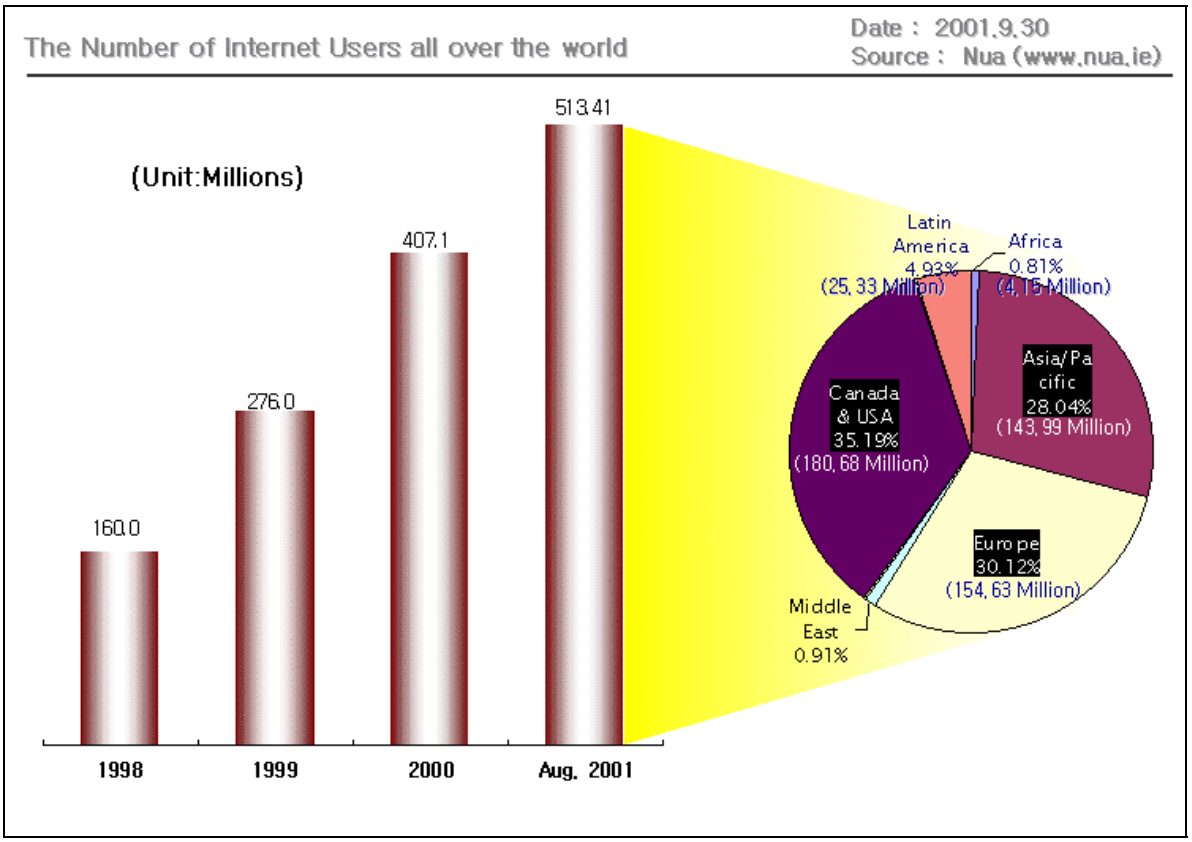
To illustrate this, let us take a look at a predominant standard used by my employer, CobiT, a control objective framework that is popular standard in the field of Information Systems Auditing. CobiT does address Electronic Commerce; however, in little detail. Control PO 8 (Planning and Organization, process 8), entitled "Ensure Compliance with External Requirements," objective number 5 (from here on out, CobiT objectives will be denoted PO 8.5), pertains to Electronic Commerce. We must note that CobiT consists of 318 control objectives. In other words, Electronic Commerce accounts for about 1/318 of the framework (0.3%). For an advancement in technology that has the enormous potential to make such a dramatic impact on security, this is not adequate guidance. As fast as technology is changing, no framework can be complete.

jwagner74@juno.com

However, effectively auditing and securing Electronic Commerce without the guidance of a framework would be nearly impossible.

SIGNIFICANCE

As of August 2001, over 500 million users were connected to the Internet (http://www.nua.ie). By taking a conservative crime estimate of one-half of a percent—that is, if only 1 out of 200 (0.5%) are potentially malicious—then approximately 2.5 million potential intruders that may try to steal from you or your organization simply by turning on a computer. (Cullinane, 1999, page 219)



We have all done it: given a waiter a credit card, and let it out of our sight long

jwagner74@juno.com

enough for the number to be written down. I attended an Institute of Internal Auditors (IIA) seminar where this was used as a parallel to e-Commerce. I am convinced this is true—*and* false. While it is true that a waiter could easily write down a credit card number and use or sell it, it is false that the potential consequences of a one time use of the credit card number could even compare to the potential consequences of several thousand Internet bandits obtaining the number. A one time fraudulent purchase of $2,000 is far less devastating than 1,000 fraudulent purchases of $100—or even as little as $10, for that matter. Another factor to consider is that a credit card number stolen on the Internet is likely to result in blame being placed on the e-Commerce service, which damages the reputation of the organization resulting in a diminished customer base (reputation risk).

Despite the potentially devastating consequences of insecure Electronic Commerce, many businesses currently use Electronic Data Interchange (EDI) to purchase supplies and sell goods. The speed of such commerce is often much easier and less costly over the Internet. However, as the potential risks are enormous, and as e-Commerce usage will continue to grow, security tools and IS auditing guidelines will be significant mechanisms in conducting e-Commerce in a secure manner.

SCOPE/LIMITATIONS

Audit Software was not used for two reasons: such expensive software was economically unfeasible, and the lifespan of software is much shorter than that of a

control framework. Though I use several software packages in conjunction with my employment, I was unable to use the software due to licensing restraints. However, through use of such tools, I have learned that while tools are clearly a benefit to the audit process, and some tools are clearly superior to others, that the objective of their use is independent. Financial and longevity constraints created a significant limitation, and narrowed the scope of this project to predominately methodological and control objective issues. Suitable software tools have been used for graphical and analytical purposes.

The remarkably fast rate of technological change has been significant limitation of this project. Any aspect of IS Auditing related directly to software, hardware, and applications must consider that current technologies will soon be outdated. Although these control *procedures* will soon be outdated, control *objectives* remain constant. To illustrate this, let us consider CobiT process DS 5, Ensuring System Security. While system security is a control objective for both manual and automated systems, the process used to obtain this objective is very different. This has enabled the integration of older literature and methodologies into this project, to a certain extent.

RESOURCES

The quality of the literature reviewed has been reasonably good, considering the ever-changing nature of this field. Some of the most valuable resources have come directly from the Information Systems Audit and Control Association (ISACA), also

jwagner74@juno.com

known as the Information Systems Audit and Control Foundation (http://www.isaca.org). ISACA is the producer of Control Objectives for Information and Related Technology (CobiT), which has been the primary framework in this project. Other significant resources have been the Computer Operations, Audit and Security Technology (COAST); Computer Security Institute (CSI); International Computer Security Association (ICSA); and the National Computer Security Association (NCSA). As e-Commerce makes the lines between financial auditing, performance auditing, and information systems auditing very blurred, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was referenced during this project.

I have discussed IS Auditing methodology and resources with a member of the board of the Springfield Chapter of ISACA, and I attended several seminars throughout the project. Being an IS Audit Supervisor, the training I received was a significant resource.

To the best of my knowledge, there are not, and have not been any MIS projects pertaining to Information System Auditing of Electronic Commerce conducted at UIS.

METHODOLOGY AND FRAMEWORK

The primary framework to be used will be the CobiT (Control Objectives for Information Technology) approach. This framework has been chosen, not only for completeness and flexibility, but for a focus on users, as well as IS Auditors and

jwagner74@juno.com

Management. It is also the predominant framework used by my employer. The most important aspect of any Information System is the end-user. However, in many frameworks, the interest of the end-user is lacking. Particularly noteworthy is the lack of guidance pertaining to business-to-consumer (B2C) end-users (that is, the e-Commerce customers themselves). There are two primary reasons a security exposure involving customers is a significant risk: because of the lack of control over customers, and the importance of customer satisfaction to the success of e-Commerce. For these reasons, it is surprising that current methodologies and frameworks do not appear to address B2C users in sufficient detail.

END RESULT

The end result of this project is an analysis of various aspects of IS auditing as it pertains to Electronic Commerce. Three factors were paramount in the selection of issues analyzed in this project:

- the significance of the risk involved when adequate control mechanisms are not established;
- the lack of control the organization has over the issue; and,
- the lack of guidance provided by available standards.

Wherever possible, statistical methods were used in evaluation, assessment, and substantiation.

jwagner74@juno.com

Problem Statement: As information technology is incorporated into almost every aspect of an organization, as Electronic Commerce is being considered by virtually every organization, and as Electronic Commerce has the potential to dramatically alter the way we live, mechanisms are necessary to ensure control. These mechanisms include an information system auditing framework and methodology that addresses Electronic Commerce in significant detail.

jwagner74@juno.com

CHAPTER TWO – LITERATURE REVIEW

Introduction

This has been a difficult topic to research. The quality of the available literature has been reasonably good, considering the ever-changing nature of this field. There is an abundance of data on both Electronic Commerce and Information Systems Auditing; however, literature pertaining to an interrelationship between e-Commerce and IS auditing has been limited. Some of the most valuable resources have come directly from the Information Systems Audit and Control Association (http://www.isaca.org), which is also the producer of CobiT. I have also discussed IS Auditing methodology and resources with a member of the board of the Springfield Chapter, and will attend seminars of related topics. Being an IS Auditor, training I have received and continuing education requirements I have fulfilled have been a significant resource. Control Objectives for Information and Related Technology (CobiT) (2000), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) reports, Federal Information Systems Control and Audit Manual (FISCAM) (1999), Federal Information Systems Processing Standards (FIPS) (1998), Auditability and Control (SAC) (1994), and Electronic Data Processing (EDP) (Murphy, 1989) Auditing have provided useful frameworks.

jwagner74@juno.com

The Impact of Technology on Information Systems Auditing

The need for well-educated Information Systems (IS) auditors is increasing, due to the potential of technology to dramatically change organizations and business practices. IT has impacted the business environment in three significant ways (Gallegos, 1998, page A):

- IT has increased our ability to store, capture, analyze, and process tremendous amounts of information. It has also altered the production and service process.
- IT has significantly impacted the control *process*. While control *objectives* remain constant, except for control objectives that are technology specific, technology has impacted the *process* by which the system is controlled. While a control *objective* is the same regardless of whether the system is manual or automated, the control *process* is completely different for manual and automated systems.
- IT has impacted the auditing profession in terms of the skills required to perform an audit and the knowledge required drawing conclusion.

Notice how I italicized *objective* and *process*. It is crucial to understand how objectives are, for the most part, independent of technology, and that the control process depends directly on technology. To illustrate this, lets use Protecting Sensitive/Confidential Data as an example of a control *objective*. To obtain this *objective* for a manual system, the control *process* would be to physically secure the area where the data is stored. To obtain this *objective* for an automated system, the *process* would include logically securing the area where the data is stored and to control the paths through which access to the data is gained. There is no difference in

jwagner74@juno.com

the objective for each system, but a tremendous difference in the process. The process for the automated system is clearly more complex.

Also, to elaborate on the third bullet, which pertains to the knowledge required to perform an IS audit, and draw conclusions based on the information obtained from the audit, allow me to discuss briefly my experience as an IS auditor. I often find processes or instances that violated control objectives (normally, CobiT objectives are used). However, I must use my own judgment in determining whether these violations are actually weaknesses, as the scope of the audit area or a compensating control may achieve reasonable assurance, even though absolute compliance with the objective is not met. Effectively determining adequate compliance with control objectives, or compliance through a compensating control, requires an understanding of Information Systems. To illustrate this, lets use CobiT 5.9, Promotion to Production, as an example. CobiT requires that changes to a program be moved to production by a different individual than the one who made the changes. However, in a small IS project, with a limited number of individuals with IS expertise, violation of this control may not be a substantive weakness, if a compensating control exists. Compensating controls may be adherence to procedures, approval of managers, and a well documented move to production, for example. It would be unfeasible to hire additional qualified staff for an IS division just to adhere to one objective when the benefit of adherence is overshadowed by the costs. There is not a formula for

jwagner74@juno.com

determining when a compensating control is adequate, as it depends on the size and scope of the project, and the availability of resources. This requires much knowledge on the part of the auditor, as areas are often gray, rather than black and white.

Why Information Systems Auditing?

The first question to be asked about Information Systems Auditing is *Why*? Why audit Information Systems? Why is a methodology and framework important? "Since it is increasingly difficult to clearly delineate between the computer and the rest of the organization, all auditors must now be computer literate." (Oliphant, September 1, 1998, page 2) Most businesses, private or public, profit or not-for-profit, are increasingly dependent on Information Technology—in *all* organizations. As a result of this, company survival depends directly on continued IT services. Thus, IT is a concern of internal control. Computer Auditing *is* a specialization of Internal Auditing.

The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* provides the following definitions of Internal Control (Oliphant, September 1, 1998, page 1):

> "Internal Control is part of the management process. It is the actions taken by management to plan, organize and direct the performance of sufficient actions to provide reasonable assurance that the following objectives will be met:

jwagner74@juno.com

- Accomplishment of established objectives and goals for operations and programs;
- The economical and efficient use of resources;
- The safeguarding of resources;
- The reliability and integrity of information; and,
- Compliance with policies, plans, procedures, laws and regulations."

Note the words *reasonable assurance.* The term reasonable assurance is reminiscent of training I received as an IS Auditor. During this training, I was taught that recommendations for improvement must meet the following criteria (Performance Audit Manual, 1998, page 2-D):

- Are the corrections economical? Would they cost more than a continuation of the deficiencies?
- Are the other simpler, less perfect, though feasible methods available to correct the deficiency?
- Does the corrective action go to the heart of the deficiency, or just correct surface matters?
- Does the corrective action take into account why the deficiency occurred, and who was responsible for it?

In other words, Internal Control needs to be reasonable, not absolute. When is a control reasonable? Simply when the benefits overshadow the costs.

It is impossible to be specific about the scope of IS auditing. The scope has to be determined based on the environment; this is especially challenging when dealing with Electronic Commerce and electronic data interchange. However, there are

jwagner74@juno.com

specific areas of computer auditing which are independent of technology. These basic areas can be summarized as (Oliphant, September 1, 1998, page 3):

- The organizations policies and standards;
- The organization and management of the computer facilities;
- The physical environment in which the computer systems operate;
- Contingency planning;
- The operation of the system software;
- The application systems development process;
- Review of the business applications; and,
- User programming (or end-user computing).

Because IT facilities have become vital to organizational functions, clear policy statements have become a necessity. Without a clear statement of direction, organizations can become disoriented and perform ineffectively. Standards are the means by which policy is attained. The IS auditor must assess both the adequacy of the standards, and the compliance with the standards. Policies and standards are critical in the following areas (Oliphant, October 1, 1998, page 2):

- Systems development life cycle;
- Analysis and programming;
- Data structures;
- Security;
- Data controls;

jwagner74@juno.com

- Documentation;
- User procedures; and,
- User programming.

It is worth mentioning that in a technological era, where developments increase at an exponential rate, technological standards can become quickly outdated. While the objectives of control remain feasible for a longer period of time, the ways in which the objectives are met must be reviewed at a fairly consistent rate. Without strong policies and standards, "anarchy can quickly rule." (Oliphant, October 1, 1998, page 2).

Electronic Commerce

Now that I have discussed Information Systems Auditing, I will address Electronic Commerce as it relates to Information Systems Auditing. Electronic Commerce has become a significant force in the business world, mostly because of its ability to accelerate the business processes through faster orders, invoices, acknowledgments and payments. To dig a bit deeper, the effects of e-Commerce are not only speeding up the business processes, but are completely altering it. An example of this is that customers will be interacting directly with the manufacturer, and bypassing the middleman altogether.

As EDI, which is the most common method of Electronic Commerce, moves from value-added networks (VANs) to the Internet, serious security issues must be

jwagner74@juno.com

addressed. VANs are Internet-like networks used for communications between business partners. Two major issues are the security of the data transmitted, which includes both the reliability of the transaction and the security (privacy of the data); and the problem of "dropped packets." While dropping data while browsing the Web is minor, this would be unacceptable for Electronic Commerce, as the data is often highly sensitive. The most common method of securing Internet data is encryption, which is highly effective and important, but not enough as eventually, a way around it is usually discovered. Additional security measures must be in place. (Russel, 1997, page 13)

As an enormous amount of business is shifting to e-Commerce, and customers are going directly to the manufacturer, financial concerns will move toward electronic transactions. Inevitably, Certified Public Accountant's (CPAs) will have to become technically informed to adequately meet customer needs. The chairman of the AICPA, Robert Mednick, has recognized this. In his inaugural speech he stated that he "envisions an expanded role for CPAs as premier information professionals" in a world of Electronic Commerce and virtual global trade, and challenged CPAs to serve the "broad information needs of decision makers in today's information age." Clearly, AICPA Chair Mednick understands the need to keep pace with Electronic Commerce. (CPA, December 1996, page 13)

jwagner74@juno.com

Federal policies related to EDI

Electronic Data Interchange (EDI) is strongly related to Electronic Commerce, as Electronic Commerce required that data be exchanged electronically. As mentioned before, standards are essential to maintain a controlled environment. There are a few applicable federal policies that pertain to EDI; these include (CSL, 1991, page 1):

- The Computer Security Act of 1987, which requires federal departments to develop a security plan which includes:
  - Identification of EDI systems that are sensitive;
  - Preparation and maintenance of security plans for sensitive EDI systems; and,
  - Security training for employees involved in the development and operation of sensitive EDI systems.
- "Security of Federal Automation Information Systems" (Appendix III, OMB Circular A-130), a government-wide policy which contains several elements directly applicable to EDI including:
  - Security requirements that include a definition of security specifications, security testing to assure proper implementation of controls, and management certification to the adequacy of security safeguards;
  - Periodic security audits for sensitive applications; and,
  - Contingency plans to assure the continuity of essential information processing services.
- Federal Managers Fiscal Integrity Act, which require periodic internal control audits, and require that significant deficiencies be reported as *material internal control weaknesses*;
- Requirements for the Management of Electronic Records (issued by the National Archives and Records Administration (NARA) as 36 CFR Part 1234), which

jwagner74@juno.com

mandates an effective electronic records security program and states the electronic records may be admitted as evidence in federal court proceedings if trustworthiness is established through thorough documentation of IS operation and controls imposed upon it; and,

- OMB Circular A-127, which requires policies and procedures be followed by executive departments to develop, operate, evaluate, and report on financial management systems.

Clearly, the government is becoming very interested and active in protecting the integrity of electronic data.

Increased use of e-Commerce correlates negatively with the use of paper documents and manual signatures. Consequently, documents remaining in electronic form and the growing use of digital signatures create new risks that must be considered in any Electronic Commerce system.

The lack of hardcopy documentation is both a significant advantage and a substantial vulnerability of EDI. While ability to organize and access large amounts of information, and speed of transferring logical data as opposed to physical data are clearly better with and electronic data system, the issue of maintaining data integrity becomes more complicated. Hardcopy evidence may not be available, and an intruder no longer needs physical access to obtain, modify or destroy such documentation; this can be done from a remote location. In addition, more data can be altered much faster with computer technology. Steps must be taken to ensure data is authentic, accurate, secure, and that there is an appropriate audit trail for purposes of accountability.

jwagner74@juno.com

Audit Considerations

EDI presents a new challenge for internal auditors. Hardcopy records and signature authorizations are not always available, and “auditing around the computer” is not feasible. All auditors must demonstrate technical understanding. When reviewing controls over EDI, auditors should consider documentation, policies and procedures, testing and maintenance. In addition, segregation of duties, appropriate access authorization, error detection/correction/protection, and determine whether there is an adequate audit trail. With high dependence on IS, backup, disaster recovery, and legal agreements for backup and disaster recovery are important areas to be reviewed. (SAC, 1994, page 8-89 through 8-92). As EDI and e-Commerce present significant risks, both to the security of data, and to the ability of and organization to perform its functions, the line between IS auditing and all other types of auditing is becoming increasingly blurred.

jwagner74@juno.com

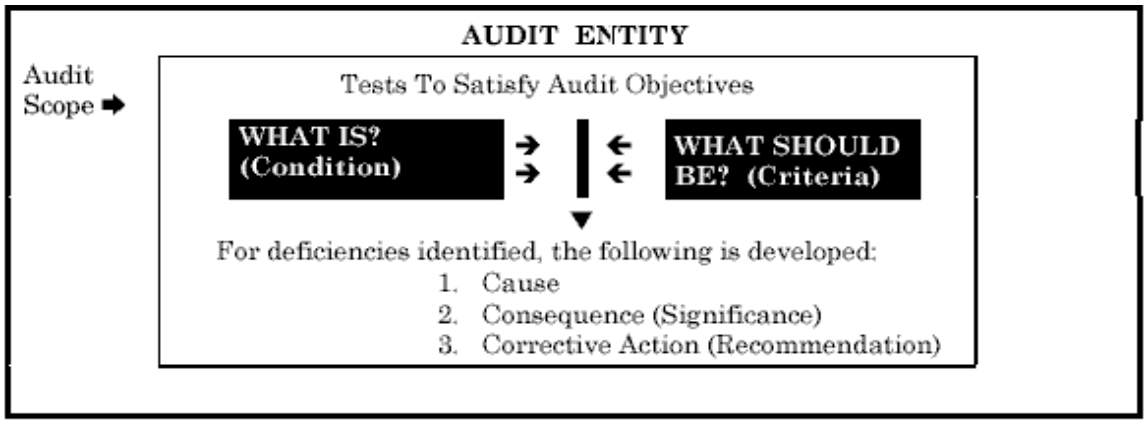
CHAPTER THREE - METHODOLOGY DEVELOPED

As Electronic Commerce is being considered by virtually every organization, and has the potential to dramatically alter the way we live, mechanisms are necessary to ensure control. An IS auditing framework which meets this need is lacking. While there is an abundance of data on both Electronic Commerce and IS auditing, information pertaining to the interrelationship between the two is scarce.

The process of developing this project was three-fold:

- First, this project entailed an analysis of common and significant deficiencies in the auditing of Electronic Commerce. The analysis included an identification of an audit concern, an evaluation of the control the organization has over the concern, and an assessment of the risk incurred by the audit concern.
- Secondly, this project involved determining issues that were not adequately addressed by existing methodologies and frameworks.
- Finally, this project will involve compiling Supplemental Control Practices to address the needs not met by existing methodologies and frameworks.

I am confident that this project has began building a bridge between the "what is" and the "what should be" of Electronic Commerce audit and control.



(Performance Audit Manual, 1998, page 1-D-1)

Graphs, diagrams, and other appropriate visual aids have been used to portray the relationships between aspects, issues, entities, and processes involved in the IS auditing process. The end result is in thesis/methodological and control objective format.

The primary frameworks used during the course of this project were CobiT (Control Objectives for Information Technology), COSO (Committee of Sponsoring Organizations of the Treadway Commission), FISCAM (Federal Information System Control Audit Manual), and FIPS (Federal Information Processing Standards). CobiT is not an IS auditing methodology; it is a "framework of generally applicable and IS and security control practices for information technology control." (Colbert and Bowen, 1998, page 2)

Although most methodologies and frameworks do not address Electronic Commerce in depth, other objectives have provided applicable control issues for Electronic Commerce. As previously mentioned, control *objectives* do not change at a rapid rate. For this reason, older control frameworks and literature can be integrated to a certain extent. It is also valuable to understand older materials (even materials that may be outdated) for one justifiable reason: an understanding of why a control objective has changed is important in not repeating a mistake. For example, older versions of EDP Auditing recommend that security administrators assign strong passwords that

jwagner74@juno.com

cannot be changed, with the logic being to prevent users from selecting poor passwords. However, now it is recommended that users select their own passwords, and change them periodically. The logic behind this is that not even an administrator needs to know another user's password; this is especially true in an e-Commerce environment, where even an administrator could exploit the capabilities that come with passwords protecting sensitive information. Understanding why reputable standards change is important so that the mistake may not be repeated.

System Auditability and Control (SAC) and Electronic Data Processing (EDP) Auditing have been additional frameworks used in understanding control issues, primarily for their focus on the IS Auditor, Internal Auditor, and Management. While these do not discuss Electronic Commerce directly, objectives pertaining to data security and external threats were applicable. However, these frameworks were not reported in the analysis of existing methodologies because they are outdated.

SAC (1994) consists of 1193 pages in 12 modules, and discusses processes, subsystems, and people. The primary users of SAC are Internal Auditors. (Colbert 1998, page 2). Three components of internal control are the environment, the system (manual and automated), and the control procedures. SAC classifies control in five ways: preventative/detective/corrective, discretionary and non-discretionary, voluntary and mandated, manual and automated, and application and general controls. While SAC does not mention Electronic Commerce, Appendix A of SAC Module 8 is

jwagner74@juno.com

dedicated to Electronic Data Interchange (EDI), which is directly related to Electronic Commerce. Electronic Data Processing (EDP) Auditing will not be used to the same extent as other frameworks. However, EDP's detailed descriptions of several audit areas, particularly the areas pertaining to data security, have been useful in gaining understanding. As mentioned previously, objectives are highly independent of technology, which allows EDP to be a useful supplement to the other methodologies and frameworks used during this project.

Through an ISACA listserver, I came into contact with a private information systems audit director, who referred me to *Millers Electronic Commerce Assurance Services*. (Nagel, 1999) While this document is not a methodology, it is devoted to Electronic Commerce, and discusses auditing in some sections. As CobiT, COSO, FISCAM, FIPS, SAC, and EDP Auditing do not discuss Electronic Commerce in detail, Miller's Assurance Services has been a valuable aid in understanding Electronic Commerce.

While this project has involved a review of several methodologies, and a utilization of applicable control issues presented in each of the methodologies, this project will entailed an identification of Electronic Commerce control issues, and a determination of lacking control objectives in existing methodologies. An example of an instance where a control objective is lacking is CobiT PO 8. Objective PO 8.5 addresses Electronic Commerce. However, confidentiality and integrity are not cited as

jwagner74@juno.com

information criteria for this control objective. Clearly, the confidentiality of sensitive information as it is transmitted via electronic data interchange (EDI) should be a control concern.

Methodology for Analyzing Control Issues and Reporting Results

Electronic Commerce control concerns were identified, the amount of control the organization has over the issue was evaluated, the risk the control issue presents to the organization was assessed, the adequacy of existing control frameworks was evaluated, and suggested supplemental control practices were developed. The analysis and results for each audit concern have been presented in the following format:

- Audit Concern;
- Organizational Control;
- Risk Assessment;
- Existing Standards; and
- Supplemental Control Practices.

Definitions for each area analyzed and presented are as follows:

Audit Concern: The audit concern will be documented and justified.

Organizational Control: The amount of control the organization has over the audit concern will be evaluated. To aid the audience of this project in understanding the control issues, areas where the organization has control will be denoted by thumbs-up

jwagner74@juno.com

bullets (👍) and areas where the organization lack control will be denoted by thumbs-down bullets (👎). The overall control the organization has over the concern was rated as high, medium, or low.

Risk Assessment: The risk the audit concern presents, including the likelihood of occurrence and degree of consequences, will be assessed. An Impact/Exposure Coefficient was useful in assessing risk (see Appendix 4). As several factors impact risk, and as risk can vary in different environments, it is difficult to formulate a method for assessing risk. Therefore, the overall risk will be assessed as high, medium, or low.

Existing Standards: Prevalent standards certified or published by a reputable organization will be reviewed, and their strengths and shortcomings discussed. The sufficiency of existing standards will be rated as adequate, fair, or inadequate.

Supplemental Control Practices: Supplemental Control Practices will be suggested. Initially, it was my intent to develop a standards framework or methodology to secure Electronic Commerce. Through research, I have determined that it is best to call the results Supplemental Control Practices. The reason for this is two-fold:

1. Standards, frameworks, and IT audit methodologies are typically certified by a reputable audit organization. This is not the case for this project, and I am not qualified to certify control practices as a standards framework or methodology.

jwagner74@juno.com

2. It is not my intention to replace existing standards; the intention is to compensate for control issues not adequately addressed. There is no benefit in addressing what is already adequately addressed in existing standards certified by a reputable audit organization.

When gaps are identified, Supplemental Control Practices will be recommended with the intention of complimenting, not replacing, existing certified standards.

Conclusion

In short, each audit concern identified will be accompanied by a justification, control evaluation, risk assessment, and a discussion of the strengths and shortcomings of applicable control standards. Following the evaluation of each audit concern will be a listing of suggest supplemental control practices which are intended to assist auditors, managers, and security professionals in controlling and securing Electronic Commerce.

jwagner74@juno.com

CHAPTER FOUR - RESULTS

INTRODUCTION TO THE RESULTS OF THE PROJECT

For the most part, IS control methodologies are developed with the auditors as the primary audience. The reason for this is clear, and justifiable—the auditors are the primary users of any audit and control methodology or framework. However, it overlooks the primary foundation for any e-Commerce or IS auditing function, which is senior management. The reason for this is simple—management makes the decisions regarding resource allocation, organizational structure, and an established Internal Audit function. I personally participated in the assessment of an entity that had no internal audit function, and the head of the entity stated that "resources were best used to looking at what could be done in the future, rather than looking at what has already been done." The entity head also stated that biannual reviews, such as audits and vulnerability assessments (penetration tests), were compensating controls.

I respectfully disagreed with the entity's position because it appeared shortsighted. While one can make a logical case for focusing resources on the future rather than the past, the problem with biannual reviews and vulnerability assessments is that they are post-audit functions, which means that the mistakes are detected rather than prevented. Often, detective controls can result in a repeat of the process; or worse, a situation where the implementation, or other implementations built on top of the errant implementation, have become such an intricate part of the business, that it is

jwagner74@juno.com

nearly impossible to correct them without a severe disruption in the business process.

Allow me to illustrate this with a scenario (based on events I have witnessed, read about, or heard about during training) that could very possibly occur:

- An organization begins serving its customers via the Internet, and has to decide how to authenticate customers and protect information.
- The president of an organization, who does not understand specifics or technology, makes decisions regarding resource allocation, encryption, and data storage. His priorities are keeping the cost low, and the system easy for customers to use, because in his view the way to attract customers is to be affordable, user-friendly, and convenient.
- The organization implements a system allowing short passwords, so they will be easy for the customer to remember.
- An inexpensive, fast processing, masking algorithm is used to protect customer passwords and account information. This reduced the initial cost to implement the system, and puts less strain on processing resources because the masking algorithm worked very quickly. In addition, passwords could be unmasked by the organization, and conveniently emailed to customers when they forget them.
- Due to its ease of use, a large customer base is built very quickly. Very soon after implementation, the organization has more customers and a much higher profit margin than less user-friendly competitors.
- Someone with malicious intent towards the organization, perhaps a disgruntled former employee or an Internet thief, hacks into the organization's system, and gains access to sensitive information because default passwords had not been changed. Since the organization has not established an Intrusion Detection System (IDS), the intruder goes undetected.
- Passwords on the organization's system are easily unmasked, and the intruder can use them to obtain customer credit card information. The intruder exploits the information, by using it and selling it. Customers find unexplained charges on their credit card bills.

jwagner74@juno.com

- The organization contacts the authorities attempting to catch and prosecute the intruder. Customers hear through the press (newspapers, Internet media) that credit card information was stolen from the organization.
- Several customers withdraw their business from the organization.
- The organization implements a more secure system. This results in a disruption of service to remaining customers, and the organization expends a great deal of resources in the process.
- The organization fails to regain their reputation after the incident, and competitors gain a larger customer base and profit margin.

The scenario described above could have been prevented if a qualified internal audit function was involved in the development of the e-Commerce system. Even if a post-audit review or a vulnerability assessment would have identified weaknesses before an intruder exploited them, an unnecessary cost and disruption of service may have been incurred. In an actual incident, the prices of television sets was misstated as about $4.75 each on an e-Commerce site, and several customers were disgruntled when the organization canceled the sale (Hayes, September 13, 1999, http://www.computerworld.com). In scenarios such as the ones described above, a devastating risk taken was that of "reputation risk."

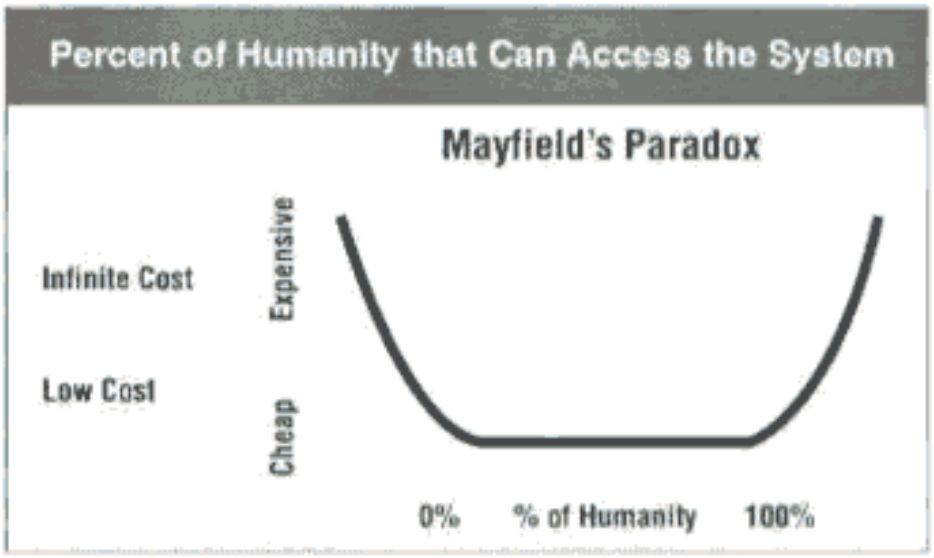
While the organization enjoyed short-term success, a poor process resulted in long-term disaster. This can be illustrated graphically in a model I have developed; I call this model "The Paradox of e-Commerce Security." Before I explain this model, I must first introduce "Mayfield's Paradox." It is through studying Mayfield's Paradox that the idea of the Paradox of e-Commerce Security came to me.

jwagner74@juno.com

Mayfield's Paradox

Mayfield's Paradox states that *"Keeping everyone out of an information system requires an infinite amount of money and getting everyone onto an information system requires an infinite amount of money, but the costs between these extremes are relatively low."*

Mayfield's Paradox (University of New Haven Center for Cybercrime and Forensics Computer Investigation, 2001, http://www.isaca.org) is depicted as a U-curve:



While examining Mayfield's paradox, I began comparing it to actual systems I have used. A system with sensitive information in it would be on the side of the U-curve which illustrated incurring great expense to keep people out. A system containing

jwagner74@juno.com

information that an entity wants to make available to everyone would be on the opposite side of the curve, incurring great expense to support as many users as possible. Then I pondered the following question: "Where on this curve would an e-Commerce system be?" (University of New Haven Center for Cybercrime and Forensics Computer Investigation, 2001, http://www.isaca.org)

One unique aspect of e-Commerce is that a perfect e-Commerce system would be on both sides of Mayfield's U-curve. Just like any other customer-oriented, profit-driven company, an e-Commerce system desires as many people (specifically, customers) having access to the system as possible. However, in doing so, an e-Commerce system deals with a great deal of sensitive data (such as credit card numbers), and therefore desires that as few people have access as possible. The U-curve illustration of Mayfield's Paradox laid the conceptual foundation for what I call the Paradox of e-Commerce Security.

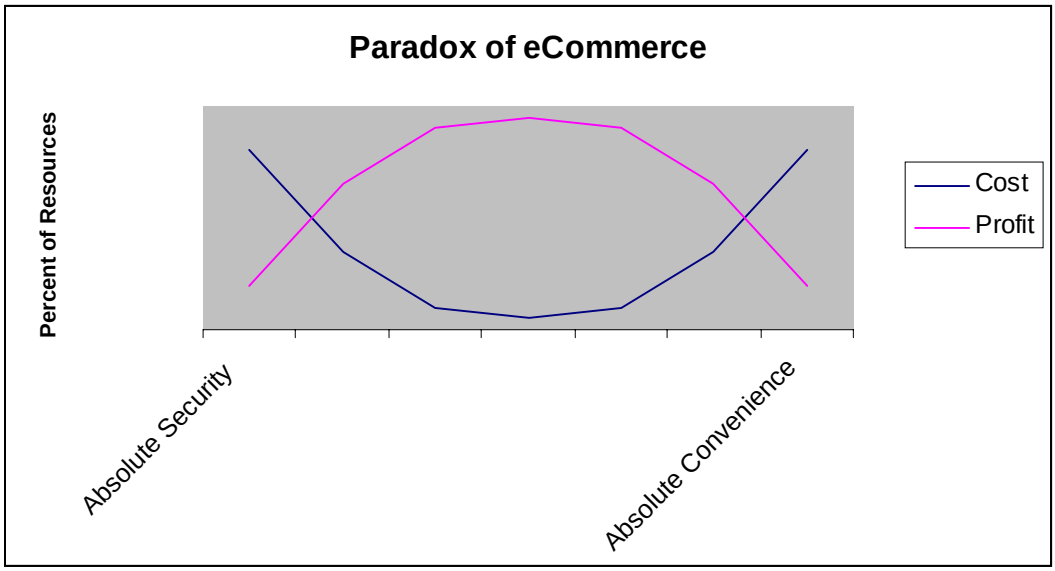
The Paradox of e-Commerce Security

As previously stated, Mayfield's Paradox states that "keeping everyone out of an information system requires an infinite amount of money and getting everyone onto an information system requires an infinite amount of money, but the cost between these extremes are relatively low." The concept behind the model I have developed, the Paradox of e-Commerce Security, is similar. The concept is:

jwagner74@juno.com

"An absolutely secure Electronic Commerce system will incur great cost and result in low profit and fail, and an absolutely convenient Electronic Commerce system will incur great loss and result in low profit and fail. Therefore, for an e-Commerce system to succeed, there must be a reasonable balance between security and convenience."

To illustrate this concept, consider the following model:



There tends to be a negative correlation between *security* and *convenience*, as an increase in one tends to result in a decrease in the other, so they share the x-axis. At one end there is absolute security, and at the other end there is absolute convenience (user friendliness, accessibility, etc.). There are two lines on the chart: one representing the resources expended (cost) from the level of security or convenience, and the other representing the resources generated (profit) from the level of security or convenience.

jwagner74@juno.com

The y-axis illustrates the percent of resources expended or generated. Cost and profit as presented here are not merely monetary terms, and must be defined:

- *Cost* is the resources expended, including money, human resources, and reputation. *Reputation* represents the goodwill of the system, the confidence a constituent has in the organization, and therefore the willingness a constituent has to do business with an organization. A *constituent* can be any entity essential to the business process, such as customers, third party alliances, or even insurance providers.
- *Profit* is the resources generated, including money, customers, and reputation.

The Paradox of e-Commerce Security model has four zones, separated by two break-even points and a maximization point. I have named the four zones as follows: the Secure-Loss Zone, the Secure-Gain Zone, the Convenience-Gain Zone, and the Convenience-Loss Zone. The names are simply derived from the priority of the system and whether the efforts result in gain or loss.

Clearly, the extreme ends of the spectrum in one of the two Loss Zones are the least desirable areas for an organization to fall within. In the middle of the model are the two Gain Zones, which are desirable yet incur different types of risks.

The Loss Zones

The two Loss Zones are poorly managed, yet fail for very different reasons. One fails because it is hard to use, and the other fails because it is easy to exploit.

jwagner74@juno.com

The *Secure-Loss Zone* illustrates an e-Commerce system that is close to impenetrable. Passwords are strong, encryption is near impregnable, software and hardware is state of the art. The organization may go as far as require customers to use two tier authentication, such as passwords and biometric devices (like thumb or retina scanners) to ensure authentication. However, the system fails due to excessive cost. The cost of implementation and maintenance is extremely high, and the system has a reputation of not being user-friendly. Customers are required to remember very long and cryptic passwords, and perhaps purchase additional equipment to use the system. The system is so careful to ensure security that customers, who do not realize that these measures are intended to protect them, get frustrated and decide to take their business elsewhere.

The *Convenience Loss Zone* represents an e-Commerce system intended to be so user-friendly that everyone wants to use it. Poor passwords are allowed, sometimes allowing blank or stored passwords. Forgotten passwords are easy to recover. It is very easy to be authenticated as a valid user. The organization may use technology to track customer habits, in an attempt to gain a competitive edge by providing advertisements appealing to a consumer profile, which could result in customers feeling their privacy has been breached. Costs incurred in developing and maintaining the system are kept low, in an attempt to gain a competitive advantage through lower prices. However, passwords are easily guessed or cracked, the system would be difficult to recover from a

jwagner74@juno.com

disaster, service disruptions can be severe, fault tolerance is low, and information on the system is not adequately protected. Once information is lost through a disaster, passwords are guessed or cracked, service is disrupted, consumers believe privacy is being breached, or an intruder gains access, constituencies lose their confidence in the system, and do not trust it well enough to use it.

The Gain Zones

The Gain Zones fall in the middle of the model, between the two break even points. While the maximization point would appear to be the desirable place to fall, it would be difficult to determine that point, and as technology and business changes, it would be difficult to stay there. The Gain Zones both are profitable, but entail different risks, and are the result of different priorities.

The *Secure-Gain Zone* illustrates an e-Commerce system where profit exceeds costs, but maximization is not achieved due to costs related to security. Customers are not as satisfied with the system's user friendliness, and administration of the system results in higher overhead, which results in higher costs of service to customers. Customers may leave in favor of a cheaper, more user-friendly competitor. However, the customer base maintained will generally be more security conscious, and reputation risk is lower. This zone provides profits, while at the same time provides a secure system and protects its reputation.

jwagner74@juno.com

The *Convenience-Gain Zone* is where profits exceeds cost, but maximization is not achieved due to costs related to disruptions and reputation. Some customers do not use the system due to some security incidents (such as intrusions or disruptions) that have diminished their faith in the system. The e-Commerce system must also deal with customers that are not security conscious, and are willing to use poor passwords, not protect their own information, etc. A significant risk of such a system is a security incident due to a customer's mistake or lack of awareness, which gets blamed on the organization. For example, a customer always uses the same password for their accounts, or uses a poor password (such as their last name), and it is disclosed; the user may sue the organization, and other customers lose confidence and withdraw their business. This zone provides profits through making the e-Commerce Service easy to use and keeping the costs low, but does so at the risk of their reputation.

Relating the Paradox of e-Commerce Security Model to IS Auditing

Either of the Gain Zones carries with it the potential to slide into one of the two loss zones, due to the different risks taken. IS Auditing itself is a security-related expense. The Paradox of e-Commerce illustrates that a perfect system cannot exist, and one must consider the factors involved, and priorities must be established. Failure to set priorities, and failure to make sacrifices on one side of the curve or the other will most likely result in failure. To quote a proverb, "if you try not to lose anything, you end up losing everything." Auditors, security administrators, senior management, and even

jwagner74@juno.com

users must understand that there are tradeoffs, and a reasonable balance must be established.

Limitations

This introduction is meant to illustrate the significant challenges incurred when developing a good e-Commerce strategy, and in developing audit findings and making recommendations. An effective e-Commerce system will not satisfy everyone, and every decision made results in risk, in one form or another; therefore, there will be tradeoffs in decision-making. The Paradox of e-Commerce model I have developed is meant to illustrate these tradeoffs, but comes with some limitations that must be considered.

The model may lead one to believe that the relationship between security and convenience is an exact negative correlation. While the two attributes tend to be inversely proportional (an increase in one tends to result in a decrease in the other), this correlation is not absolute. Similarly, the model may lead one to believe that the cost and profit factors are in an exact negative correlation, which tends to be the case, but the correlation is not absolute.

Additionally, the model may lead one to believe there is always a single point on the curve through which profits are maximized and costs are minimized. The curve would most likely be skewed in such a way that the place on the chart where profits are

jwagner74@juno.com

maximized is at a different place than where costs are minimized. The model is depicted in its simplest form, a perfect U-chart, to illustrate the relationships and tradeoffs. As with any business, an e-Commerce systems profits and costs are affected by several factors including the market, laws, technology, and customer base. The cost and profit lines on the chart will most likely be skewed, and look different for each entity graphed.

Direction of the Project

Auditing itself is a security-related expense, and the first step in having an effective e-Commerce auditing function is to establish the function. The primary audience of any control methodology is the auditor who is applying the objectives; however, the first audience must be senior management. The reason that the first audience must be senior management is because senior management must recognize the need for an audit function, and view it as an essential security factor rather than an inhibiting control and expense. One prominent Chief Executive Officer (CEO) stated "controls impede progress." While it is true that controls will slow implementation (a short-term goal), controls reduce the risk of mistakes and failures resulting in a more effective business process (a long-term goal). Auditing must be seen as such a control. As most methodologies and control frameworks have been developed with the auditor as their audience, this project will also present the need for an audit function to management.

jwagner74@juno.com

This project has addressed the relationship between the organization and users (primarily customers) in great detail. Users are still the biggest threat to Information Systems security, because the most common way systems are breached is through user mistakes (carelessness or social engineering, for example). This is even more true with an Electronic Commerce system, because the organization lacks control over the majority of users, which are customers. Current methodologies and standards provide a great deal of information on dealing with users within the organization, and in dealing with contractual users (such as outsource agreements and business-to-business (B2B) relationships). However, standards that deal with a customer's responsibility for security are lacking.

Additionally, systems development will be discussed from the perspective of auditing. Post-audit reviews, such as penetration tests, vulnerability assessments, and post-implementation reviews are important. However, a post-audit review will merely reveal mistakes that have already been made. Auditing is more beneficial if it is a pre-audit and co-audit function because it prevents many errors before implementation which mitigates the cost of implementing and repairing the error, and reduces the risk of a vulnerability being exploited before the organization detects it. It is important to address auditing and security issues before it is implemented, since when it is implemented an organization loses control.

Internet communication is an essential issue, since it is the means by which most

jwagner74@juno.com

e-Commerce systems facilitate business and interact with users (particularly customers). However, using the Internet results in limited control over transmission. As how data is physically transmitted is beyond the organization's control, a compensation is necessary. Cryptography is the most common compensation, but the mere encrypting of data is not enough.

Conclusion

The most significant risks in e-Commerce tend to be simple in concept. Establishing an effective security function, securing passwords, dealing with customers, keeping information confidential, encryption, developing secure systems, and using the best technology may seem simple in concept, but are surprisingly complex to implement. An auditor should understand an e-Commerce function both increases risks and decreases control, and should be involved in every aspect of an e-Commerce presence to ensure reasonable assurance.

jwagner74@juno.com

CHAPTER FOUR - RESULTS

INTRODUCTION TO THE CONTROL DOMAINS

I identified several control domains, based on risk and control, and developed Supplemental Control Practices to compliment control areas where current standards fell short. The final results address eight specific control domains:

- AE - Audit Establishment
- BC - Business-to-Consumer Users (Customers)
- PC - Process Continuity
- SA - Security Architecture
- SD - Systems Development
- TS - Transmission Security
- LI - Laws an Investigations
- VE - Virtual Ethics

Now, I will justify each domain selected, and summarize their significance.

AE - Audit Establishment This area was necessary because auditors, who are normally the audience of a control objectives framework/methodology, do not have control. Organizational control, however, is high because senior management has the authority. Establishing an e-Commerce auditing function is not sufficient; the function needs to contain the skills necessary to perform the function effectively. One can no longer separate accounting, laws, and computer processing. Having just CPAs,

jwagner74@juno.com

or just CISAs, is not sufficient. A mix of skills, from information security to accounting, and even legal expertise, is necessary for an audit function to protect an e-Commerce presence.

BC - Business-to-Consumer Users (Customers) Of the eight control domains, I rate this as the most critical. Customers are essential to the profit, and therefore the success, of an e-Commerce presence. However, customers no longer simply just pay for products and services; they are now actual users of the system, and as internal users, they are a significant risk. I emphasize the importance of treating them as users, rather than mere customers; however, it is not feasible to implement the same security practices as would normally be enforced over users. It is critical to the success of the e-Commerce presence that these users be satisfied using the system, while at the same time reasonable security must be enforced. As illustrated in the introduction to Chapter 4, there must be a balance.

PC - Process Continuity My research indicated that business continuity and disaster contingency efforts are different for an e-Commerce system than for other Information Systems, such as Local Area Networks (LAN). A unique aspect of an e-Commerce presence is the concept of a *reputation disaster*; and to complicate matters, a reputation disaster does not have to directly involve the e-Commerce presence. Much like how an airline disaster will have a negative impact on all airlines, a virtual disaster involving Electronic Commerce will negatively impact the e-Commerce

jwagner74@juno.com

industry as a whole.

SA - Security Architecture This domain is not unique to e-Commerce, yet it is more critical. A poor security architecture is a vastly greater risk when it is expanded to an area (in this case, the Internet and the virtual market), where there is a greater potential for security exploitation and diminished control.

SD - Systems Development This domain is not specific to Electronic Commerce, but it is more critical. It is related to SA - Security Architecture, but is focused on a smaller segment of the process. The need for a strong systems development methodology is increasingly critical for e-Commerce developments/modifications for several reasons: the criticality of the developments/modifications to the organization, increased potential for the exploitation of mistakes, the difficulty of implementing fixes, and the potential for a service disruption (which is related to PA - Process Continuity).

TS - Transmission Security When using e-Commerce, on of the greatest risks is that sensitive, and potentially destructive data, will be transmitted on a path which is beyond the control of the organization. Trusted paths (such as dedicated lines) are no longer feasible, and the Internet for many is the only choice; therefore, the only security option is to secure the data rather than the path. While current methodologies do address this, they do not consider other factors which complicate the issue. Examples of such factors are government, laws (such as encryption and export

jwagner74@juno.com

restrictions), and tax regulations (which vary greatly depending on where the data is transmitted from, and where it is transmitted to).

LI - Laws an Investigations As e-Commerce increases the scope of a business process, it can no longer be restricted to one jurisdiction. Additionally, laws are likely to change as e-Commerce becomes more popular. Tax rates may change, and even vary in states and districts. Additionally, in response to the September 11, 2001 attacks, the government is considering further laws and monitoring of Internet transmissions, which could most definitely impact the e-Commerce process. As illegal activities may occur in areas where the organization has no control, coupled with the potential for crime to occur in multiple jurisdictions, investigating incidents is increasingly complex.

VE - Virtual Ethics A major theme in COSO training I have attended is "doing the right thing when dealing with customers." Often, doing the right thing costs a lot. However, not doing the right thing can cost more in the long-term. With Internet communications, and e-Commerce, comes the potential to obtain, use, and even misuse a great deal of information about customers. There may even be laws in this area soon; for example, the GAO audited the information collecting practices of federal agencies (such as the use of cookies and web logs), and the Illinois General Assembly mandated a similar audit for state agencies. With or without laws, however, an e-Commerce organization must carefully examine what information

jwagner74@juno.com

about users should (and should not) be collected, and must be careful about how such information is used. The misuse of information tracking capabilities to gain a competitive advantage can backfire, which could devastate reputation.

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION AE – Audit Establishment

Audit Concern: A qualified independent audit function should be involved in the planning, development, design, implementation, maintenance, and monitoring of an e-Commerce presence.

Organizational Control: High.

- Senior management has the authority to establish an independent audit function.
- Auditors have no authority unless their function is established by senior management.

Risk Assessment: Medium.

- While senior management has the authority to establish an independent audit function, management is not always aware of the risks involved in not establishing an independent audit function.
- An audit function may be viewed by senior management as an inhibiting factor because it slows down the process.
- An audit function may be viewed by senior management as an unnecessary expense because qualified auditors are expensive, and in the short-term senior management may see other investments as more profitable.
- Senior management may not understand that involving an independent audit function throughout the process (from development to production) protects against mistakes that could result in long-term expense or disaster.
- Post-implementation reviews such as annual vulnerability assessments may be viewed as adequate compensations for an internal audit function, but do not prevent vulnerabilities from being implemented. While such reviews are essential, they detect vulnerabilities after they have been made exploitable when implemented.
- Auditors may not have the necessary qualifications to assess a full-blown e-Commerce presence.

jwagner74@juno.com

Existing Standards: Fair.

- CobiT M4 – Provide for an Independent Audit – CobiT addresses the need for an independent audit, and how to conduct an independent audit. CobiT also addresses the need for competence.

- COSO addresses the need for an independent audit function, but not in the detail that CobiT addresses it.

- Securing Virtual Enterprises (Marcella, 1998) Ten Steps to Success in e-Commerce, step 3 (see Appendix 5) states that technology needs to be viewed as a strategic enabler instead of a cost center. Similarly, the view of a built-in e-Commerce audit function as a control to mitigate risk/threat instead of an impeding cost is necessary.

While post implementation reviews (such as vulnerability assessments) are essential, they are incapable of detecting security exposures prior to implementation. An independent review through each phase of the process may be costly, and slow down development, but can prevent long-term exposures and mitigate risks. Most auditors are aware of this, but this is an area where auditors have minimal control; the primary audience for this area must be senior management. When an organization's profit is driven by e-Commerce, there should be a qualified, independent audit function. Most auditors in e-Commerce tend to be Certified Public Accountants (CPA); however, this is not sufficient. CPAs are critical to the success of an e-Commerce audit function; however, security professionals such as Certified Information Systems Auditors (CISA) and Certified Information Systems Security Professionals (CISSP) are necessary for the IT aspects of an audit. Additionally, having a lawyer on the audit team may be wise to protect the organization from violations of the law.

Supplemental Control Practices: Senior management should consider the following supplemental control practices over the establishment of an independent audit function:

AE.1 - An independent audit function should be established, and report directly to senior management.

AE.2 - An established independent audit function should be involved in every phase of an e-Commerce process including planning, design, development, testing, implementation, maintenance, and monitoring.

jwagner74@juno.com

AE.3 - The audit function should employ\ team members with the combined skills necessary to adequately assess all aspects of the e-Commerce process. Such skills should include, but are not limited to: accounting expertise (CPA), IT expertise (CISA), security expertise (CISSP), legal background, and telecommunications expertise.

AE.4 - The mission of the e-Commerce audit function should clearly state that the purpose of the function is mitigate the risks/threats incurred by an e-Commerce presence; the short-term costs of an e-Commerce function should be recognized as a control to achieve long term success.

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION BC – Business-to-Consumer (B2C) Users (Customers)

Audit Concern: Transactions, relationships, and dealings with Business-to-Consumer (B2C) users (customers) should be sufficiently managed; there must be a reasonable balance between the convenience allowed and the security enforced over a consumer presence.

Organizational Control: Low.

- e-Commerce organizations have limited control over the activities of users, as B2C users are the customers; as customers, B2C users chose the organization, rather than the organization hiring and training such users (as opposed to internal users that are organizational staff).

- As B2C users are customers, it is essential that the organization attract such users; therefore, generally acceptable security practices regarding the control and education of users (such as CobiT DS.7) are not feasible practices.

- As B2C users are customers, it is essential that the organization maintain a positive relationship with such users; therefore, the disciplinary measures normally associated with user misconduct are not feasible.

- As B2C users (customers) do not interact with organizational staff (as they would if they purchased goods by physical appearing at a store), standards business practices of customer authenticity (such as photo identification) are not applicable.

- Although control over B2C users (customers) is low (as such users cannot be formally controlled, hired, screened, or trained), the B2C users choose the relationship; therefore, the organization may influence and educate B2C users informally.

Risk Assessment: High.

- As B2C users (customers) are not hired, screened, or formally trained, they may pose a threat to security through a lack of awareness. User mistakes are currently the most common way security is breached (Network Security Conference, 2001).

jwagner74@juno.com

- Security incidents involving B2C users, even through no fault of the organization, can damage organizational reputation.

- Inadequate security over a B2C user presence can damage organizational reputation.

- Excessive security over a B2C user presence can damage customer satisfaction. (For example, if users are required to use excessively long, cryptic passwords, in addition to biometric devices, in order to do business with the organization, they may not be concerned with the level of security, and may leave for are more user friendly provider.)

- Litigation between a B2C user (customer) and the organization can damage organizational reputation.

- B2C users (customers) are more difficult to identify.

- Control in regards to B2C users (customers) is more than internal control – it also involves external control, which means minimal control.

Existing Standards: Insufficient.

- CobiT DS.8 – Assist and Advise Customers – addresses a help desk function, customer registration, customer queries, and trends. However, customer accounts (B2C users) are not addressed.

- CobiT DS.7 – Educate and Train Users – addresses user awareness, but is directed toward internal users. B2C users cannot be treated in the same manner as internal users.

- COSO discusses serving customers and constituents, but does so from the perspective of internal control. B2C users are external.

- Miller's Electronic Commerce Assurance Services addresses business-to-consumer WebTrust (Nagel, page 654), but not B2C relations.

- Enterprise Best Practices (Deloitte & Touche) addresses authenticity (pages 21-26), availability to users (pages 37-39), and privacy (page 32); all of which are essential to B2C e-Commerce. Additionally, Enterprise Best Practices states that "there should be communication from vendors to customers about the level of security in an e-Commerce presence" (page 44. See also Appendix 3).

jwagner74@juno.com

Surprisingly, prevalent methodologies and frameworks, even those publications directed specifically at electronic commerce, do not adequately address the most significant risks related to e-Commerce customers. e-Commerce customers are more than individuals who walk into a store and purchase an item—they are actual users of the system with user ids and accounts. Being a user gives them the power to be a security exposure. For this reason, e-Commerce customers have been called *B2C users* because they have an actual role in the organization—to view them merely as a customer who shows up to buy a product then leave is a grave misconception.

Security is viewed differently by many individuals, and is normally seen as either an enabler or an inhibitor. A study by Deloitte and Touche in 2000 indicated the following (Global Status Report, page 49):

- 15% believe security *enables* e-Commerce.
- 25% believe security *somewhat enables* e-Commerce
- 19% believe security *somewhat inhibits* e-Commerce
- 6% believe security *inhibits* e-Commerce
- 35% believe security *neither enables nor inhibits* e-Commerce

The good news is that of those who acknowledge as important, security is seen as an enabler (40%) more than it is seen as an inhibitor (25%). However, the bad news is most when you add those who do not see security as a factor (35%) with those who see it as a detriment, it is revealed that a majority (60%) do not see security as a benefit to e-Commerce (Global Status Report, page 49). For this reason, an e-Commerce auditor has the responsibility to ensure the e-Commerce process not only provides adequate security, but that the process involves informing constituents of why it is important to have security. Security professionals need to understand that many B2C users who do not view security as important will be the same users who will blame IT if anything goes wrong (Lundquist, http://www.zdnet.com/eweek). This unfortunate truth of e-Commerce security must not be ignored.

Supplemental Control Practices: In addition to ensuring existing, adequate control practices are followed, internal and external auditors should consider the following supplemental control practices over B2C users:

BC.1 - Policies should be in place to informally educate B2C users as to the risks of doing business electronically, and to the actions they can take to mitigate these risks.

jwagner74@juno.com

BC.2 - B2C users should be required to have passwords of a sufficient length, and be encouraged to select difficult to guess passwords, when establishing their accounts. Dictionary words should be discouraged, and commonly exploited passwords (such as "password", the user's last name, the user id itself, month names, etc.) should be forbidden.

BC.3 - After five consecutive attempts to log on to a B2C user's account, the account should be disabled, and the B2C user contacted of the incident. Sufficient information should be logged to assist in the determination of where the violation occurred, if the B2C user is not responsible.

BC.4 - B2C users should be encouraged to change their passwords quarterly; the encouragement should be accompanied by an explanation that this is important to protect the security of their account. Annual password changes should be mandatory (Nagel, 461).

BC.5 - Passwords should be stored with non-reversible encryption; no one, not even organizational staff should ever be able to obtain a B2C user's password.

BC.6 - B2C users should be informed, and frequently reminded, that no one from the organization will ever solicit them for their password. Additionally, they should be instructed to report such incidents.

BC.7 - A mechanism should be in place to ensure B2C users who forget their passwords are positively identified; standard shared secrets are useful, but not sufficient. If a B2C user is positively identified passwords should be reset, not revealed. Upon a reset, the e-Commerce application should require that the password be change immediately at the next log on. Resetting a password then forcing a change, as opposed to revealing it to the B2C user, has two primary values: 1) If a person (rather than an application) resets the password (normally a help desk), the person will not have access to the B2C user's account; and 2) if an intruder manages to be authenticated, the problem may be detected when the valid B2C user cannot access their account.

BC.8 - Options to delete sensitive B2C user information (such as credit card numbers) should be made available to users, and encouraged for casual (infrequent) B2C users. For frequent B2C users (such as businesses), this option would be inconvenient; additionally, this option may be insecure for frequent B2C users because it would

jwagner74@juno.com

increase the number of times the sensitive information is transmitted to the organization (which makes the information more vulnerable to sniffing or interception).

BC.9 - B2C users should be informed, and frequently reminded, that no one from the organization will ever solicit them for credit card (or related sensitive) information other than at the point they initiate a purchase. Additionally, they should be instructed to report such incidents.

BC.10 - Procedures should be in place to handle misconduct on the part of B2C users. Litigation can be extremely disruptive to an organization's process and reputation, and should be handled cautiously.

BC.11 - B2C user accounts should be deleted after no more than 90 days of inactivity.

BC.12 - Any time a transaction is initiated by a B2C user, the user should be notified and required to confirm the transaction.

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION PC – Process Continuity

Audit Concern: The e-Commerce process should have procedures in place to ensure the continuity of the e-Commerce process in the event of a major failure or disaster (CISSP, page 28), including a reputation disaster.

Organizational Control: Medium.

- The organization has no control over the occurrence of a natural disaster (such as a tornado or earthquake) or a service disruption.
- The organization has a great deal of control over the steps it takes to ensure recoverability in the event of a natural disaster or disruption.
- The organization can take steps to prevent events that could result in a reputation disaster (such as theft of sensitive information, public disclosure of a significant security incident, defacing of a web page visited by B2C users, etc.).
- The organization has minimal control over the steps taken by a competitor or others in the e-Commerce industry to prevent a reputation disaster; reputation disasters elsewhere in the industry may have a negative effect on the public's perception of the industry as a whole. (For example, a plane crash may hurt the corresponding airline the most, but it may turn others in the public away from flying altogether and therefore hurt the industry as a whole.)
- While the organization has minimal control over steps taken by a competitor, the organization can learn from a competitor's mistakes to mitigate risks in their own environment. (For example, airlines that were not a victim of hijacking during the September 11, 2001 terrorist attacks are also implementing additional security measures to mitigate the risks of a future disaster.)

Risk Assessment: High.

- Natural disasters are costly to ensure recovery from, and costly to recover from.

jwagner74@juno.com

- Reputation disasters are costly, and it is difficult to regain goodwill after it has been lost.

- Others in the industry, who are beyond the control of the organization, are a risk to organization's reputation.

Existing Standards: Fair.

- CobiT DS.4 – Ensure Continuous Service – adequately addresses disaster recovery, including: criticality classification, alternative facilities, backup and recovery, recovery testing, training, and risk management. However, CobiT does not address recovery from an incident damaging reputation.

- COSO does not address business continuity in detail adequate for an e-Commerce process.

- FISCAM 3.6 addresses service continuity, including the criticality of operations, damage minimization, and testing. While the concept of damage minimization is critical, FISCAM addresses it from the perspective of damage to the business process and does not consider reputation damages.

- FIPS does not address business continuity.

- Miller's Electronic Commerce Assurance Services addresses disaster recovery including rapid correction, testing, and prioritization. Reputation disasters are not addressed.

When most methodologies, standards, frameworks, or publications discuss business continuity or disaster recovery, they are usually referring to service disruptions or disasters (natural or otherwise). It seems that the concept of a "reputation disaster" is not addressed in any prevalent IS publications. If a hacker, or a disgruntled employee, changes the primary e-Commerce web site (the page through which customers initiated purchases), the perception is that security was breached. Such a breach does not mean that sensitive information was compromised; but customers would normally suspect the worse. If the organization or a competitor incurs a breach, which results in credit card numbers being exploited, some potential customers may withdraw from e-business altogether. Such virtual disasters can destroy a reputation to the point that it is the virtual equivalent of customers not even wanting to visit a store. e-Commerce carries with it the potential to make one incident a huge disaster, particularly if the media gets involved (Network Security Conference, 2001). As fast as news (and rumors) can travel across the Internet, the threat of a reputation disaster cannot be

jwagner74@juno.com

ignored.

Supplemental Control Practices: In addition to ensuring existing, adequate control practices are followed, internal and external auditors should consider the following supplemental control practices over process continuity:

PC.1 - A process continuity plan should be in place to address threats an organization's reputation, and actions to be taken to minimize the effects of a reputation disaster.

PC.2 - A well-trained, qualified response team should be established to address reputation disasters, and minimize the negative effects on the process.

PC.3 - In the event of a reputation disaster, the organization should contact B2C users (customers) to inform them of the steps being taken to address the disaster and ensure them of the safety of continuing to do business with the organization.

PC.4 - B2C user (customer) inquiries regarding a reputation disaster should be addressed promptly to maintain a positive relationship.

PC.5 - Organizational management should ensure that reputation disasters that happen to other organizations, their causes, and their solutions (especially for those within the same industry) are considered when updating and implementing process continuity plans and establishing a response team.

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION SA – e-Commerce Security Architecture

Audit Concern: The e-Commerce organization should provide a consistent plan and approach that addresses all aspects of security within an organization (Network Security Conference, 2001).

Organizational Control: Medium.

- Senior management has the authority to establish a security architecture.
- Organizations, particularly virtual enterprises, are becoming increasingly decentralized, resulting in the lines of authority becoming increasingly blurred. (Marcella page 79)
- Senior management may not realize the importance of an enterprise-wide security architecture.

Risk Assessment: High.

- The lack of an enterprise-wide security architecture results in inconsistent and poorly secured e-Commerce applications. (Network Security Conference, 2001)
- The lack of an enterprise-wise security architecture results in security exposures and exploitations going undetected.
- The lack of an enterprise-wide security architecture results in users (internal, external, and business-to-consumer users) who lack awareness, do not take responsibility for security, and are more easily exploitable.

Existing Standards: Fair.

- CobiT PO.2 (Define the Information Architecture) - CobiT discusses enterprise information standards, and developing an information architecture model, which are essential to the success of an e-Commerce organization. However, CobiT does not discuss applying the architecture to an e-Commerce presence.
- FISCAM 3.1 (Entity-wide Security Program Planning and Management)

jwagner74@juno.com

discusses and enterprise-wide security architecture. FISCAM thoroughly discusses entity-wide security planning; however, users of the entity are assumed to be internal, rather than the wider range of users involved in an e-Commerce presence.

- Enterprise Best Practices (Deloitte & Touche) states that "there should be a commonly understood set of practices and procedures to define management's intentions for the security of e-Commerce" (page 41), and that "there should be shared responsibility within an organization for e-Commerce security" (page 43). See also Appendix 3.

e-Commerce has taken off, and many entities and individuals are doing business electronically. However, we have not seen the full effects, both positive and negative, of e-Commerce on business and in our lives. Now is the time to start building security into electronic commerce systems. Architecture is a "style or method of construction" (Webster's Dictionary); similarly, an e-Commerce security architecture should be a method of virtual construction. (Network Security Conference, 2001)

To illustrate the importance of having an architecture *before* implementing e-Commerce applications, lets discuss a simpler form of architecture: buildings. How sturdy would a building be if someone hired some construction workers and told them to just start constructing a building? Not very sturdy, if they even managed to finish the building at all. Now suppose they called an architect in, and told him to strengthen the building: a near impossible task once it has been built. To build a sturdy building, and architect must first design, then oversee as construction workers build. An e-Commerce organization should follow the same logic. Auditors and security professionals should not be asked to secure an application *after* it has been built; the application should be build around an *already defined* security architecture, with auditors and security professionals involved in the process. This is true of any system, but more so with e-Commerce systems, as e-Commerce systems encounter more threats, greater risks, and limited control. (Network Security Conference, 2001)

Supplemental Control Practices: Senior management and auditors should consider the following supplemental control practices over an enterprise-wide security architecture:

SA.1 - Senior management should ensure that an e-Commerce organization has a formal, enterprise-wide, security architecture to ensure all the security and control of information assets and e-Commerce transactions.

jwagner74@juno.com

SA.2 - An Intrusion Detection System (IDS) should be in place to protect against unauthorized destruction or disclosure of data from both internal and external threats.

SA.3 - An Intrusion Detection System (IDS) should be in place, and e-Commerce processes and devices should be configured to collect as much information as reasonably possible, to facilitate the detection and correction of faults, errors, and security exploitations.

SA.4 - An e-Commerce Security Officer(s) should be assigned the responsibility for the security of an e-Commerce presence, and should report directly to senior management.

SA.5 - All e-Commerce security policies, and development/change policies, should be subordinate and adherent to an enterprise-wide security architecture.

SA.6 - The enterprise-wide security architecture should include e-Commerce security incident response procedures. (See also Chapter 4, Section PC - Process Continuity)

SA.7 - Senior management should recognize the importance of, and threats to, the security and integrity of an e-Commerce presence, and take a proactive role in assigning responsibility and ensuring security awareness.

SA.8 - All users, including business-to-consumer users, should be made aware of their roles and responsibilities in ensure e-Commerce security. (see also Chapter 4, Section BC - Business-to-Consumer Users)

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION SD – System Development

Audit Concern: A qualified independent audit function should be involved in every phase of an established systems development life cycle (SDLC) methodology.

Organizational Control: High.

- Senior management has the authority to require an independent audit function to be involved in every phase of a systems development life cycle (SDLC) methodology.

Risk Assessment: Medium.

- While senior management has the authority to require an independent audit function be involved in every phase of systems development, modification, or enhancement projects, management may see such involvement as an inhibiting factor because it slows down the development process.

- The desire to gain a competitive edge by entering a virtual market quickly may result in improperly tested and inadequately secured e-Commerce applications. Conversely, thoroughly tested and carefully developed e-Commerce applications may lose a competitive edge if not implemented timely.

- Audit findings in the monitoring/maintenance phase may be unfeasible to correct immediately.

- An improper security architecture may result in attempts to secure an e-Commerce presence after it is developed, rather than building the architecture in accordance with established security and control practices.

Existing Standards: Fair.

- CobiT PO.10 (Manage Projects) addresses each phase of systems development adequately. However, findings that are unfeasible to repair timely are not addressed. Additionally, the need to balance security with timeliness is not addressed.

jwagner74@juno.com

- COSO addresses change control, and also addresses it from the perspective of risk assessment and customer service.

- The CISSP study manual states that a candidate for the CISSP designation should fully understand the security and controls of the system development process and of the application being developed or modified to ensure data and application integrity and security (CISSP, 2001). Similarly, auditors involved in each phase of the process should have the same understanding.

- FISCAM 3.3 (Software Development) and 3.6-1 (Assessing Criticality) are related to assessing criticality and the process by which applications should be developed. However, detail is not sufficient to address the increased risk and lack of control incurred by an e-Commerce presence.

- FIPS provides detail about security of data transmissions, which should be incorporated throughout an e-Commerce system development.

A poor systems development process is often the underlying cause for security breaches and system failures. An independent audit function can mitigate such risks to security, integrity, and availability (CISSP, 2001). It is common for a system to be developed quickly to meet an unreasonable deadline, and then auditors and security professionals are assigned the task of securing the application; this is especially dangerous for an e-Commerce development, as it is remotely accessible.

I have personally reviewed a wide-area system; not an e-Commerce system, but a system involving several remote locations and Internet accessible log-in points very similar to an e-Commerce system. I am forbidden by law to disclose what I find in performing my job duties; however, I can disclose that I audited a system (this system, fortunately, no longer exists) which stored and transmitted all data (including passwords) in clear text, and default passwords were easy to guess (if you knew one, you knew them all because the convention was obvious) with no requirement to change them. No monitoring was in effect, no intrusion detection; the goal of the system development was simple: meet an "or else" deadline. The recommendations to improve the system would have been disruptive to implement; however, had the recommendations come as part of a co-audit function, they could have been built-in to the system easier. A built-in audit function may have slowed implementation, but would have been a security enabler that could have averted a serious disruption (in this case, an entire system replacement).

jwagner74@juno.com

Supplemental Control Practices: Senior management and auditors should consider the following supplemental control practices over the establishment of an independent audit function:

SD.1 - A qualified and well trained audit function should be involved in every phase of an e-Commerce development or modification process.

SD.2 - The auditor(s) assigned to the process should have the necessary knowledge to add value; appropriate education and designations (CISA, CISSP, CPA, etc.) along with training that is technologically specific to the project(s) are essential.

SD.3 - A Next Change File should be established, for findings that are unfeasible to correct timely, to ensure subsequent developments or changes result in either a fix of the finding or to avoid a repeat of the finding.

SD.4 - The systems development process should be in line with the organization's Security Architecture, which is increasingly essential for organizations incurring the amplified risk of an e-Commerce presence (see Chapter 5, Section SA for Security Architecture).

SD.5 - Vulnerability assessments of e-Commerce developments should be performed prior to implementation (to detect exposures before they are exploited in production), and periodically after implementation.

SD.6 - As e-Commerce projects are more accessible, and therefore present a greater risk than internal projects, the security, integrity, and availability of data and the application should be addressed at every phase of development, storage, transmission, or access. (This is especially important where sensitive information such as credit card numbers and passwords are involved.)

SD.7 - As e-Commerce involved the transmission of sensitive data, cryptography and authentication should be considered at each phase, and especially when data is transmitted over external networks (such as the Internet). (See also Chapter 4, Section TS for Transmission Security)

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION TS – Transmission Security

Audit Concern: There should be a means to ensure that data transmissions are secure (cannot be altered), confidential (cannot be viewed by unauthorized entities), and authentic (the identity of the sender is certain).

Organizational Control: Low.

- The organization can encrypt data transmissions, and implement mechanisms to ensure authenticity.
- As dedicated paths of transmission are unfeasible, the organization must depend on paths controlled by an external party (such as the Internet or phone lines), and therefore organizations have no control over where data transmissions travel en route to their destination.
- As the organization must depend on paths controlled by an external party, the organization has minimal ability to detect unauthorized attempts to intercept or view transmissions.
- Legal barriers exist which limit the organizations ability to protect e-Commerce transmissions. (see also Chapter 4, section LI - Law and Investigation)

Risk Assessment: High.

- Unauthorized altering or viewing of data can result in disruptions, cost, loss of reputation, and even lawsuits.
- The organization may not have the authority to investigate security incidents without legal intervention.
- If the organization does business outside of the United States, strong encryption to protect data is prohibited by law (transmissions outside the United States are limited to 40-bit encryption, which is easy to crack [Ghosh 1998, page 14]), which entails two significant risks: 1) unauthorized parties who intercept or sniff data transmissions can easily decrypt them, and 2) legal consequences may be incurred if stronger

jwagner74@juno.com

encryption travels across United States borders.

- Laws regarding the legal limits of encryption, both within the United States and across borders, are subject to change.

Existing Standards: Fair.

- CobiT DS.11 (Manage Data) discusses authentication, integrity, and transmission over the Internet. However, it does not consider legal barriers.

- CobiT DS.5 (Ensure System Security) discusses trusted paths. However, trusted paths are not normally a feasible option for e-Commerce transactions.

- Enterprise Best Practices (Deloitte & Touche) states that "there should be a means to ensure the confidentiality of data communicated between customers and vendors" (page 33). Enterprise Best Practices also discusses the lack of control over transmission paths, resulting in a need to protect the data itself. However, legal ramifications are not discussed.

- Deloitte & Touche has also developed *e-Commerce Security-Public Key Infrastructure (PKI): Good Practices for Secure Communications*, published by the Information Systems Audit and Control Foundations (ISACF) in 2001. This document is a very good technical reference, and presents useful control practices for the use of PKI, Secure Sockets Layer (SSL) and Kerberos to provide protection and authentication. It also provides very detailed, encryption specific audit programs. However, as it is technically specific information, it is not incorporated into supplemental control practices. However, currently it is an excellent method of fulfilling control objectives and security.

There are only two ways to protect information assets: control the paths by which access to the resource is gained, and safeguard the resource itself. Most e-Commerce organizations must do business over the Internet, as it is available and accessible to most anyone. However, in doing business over the Internet, controlling the path by which access to information assets is gained is difficult, if not impossible. Therefore, safeguarding the data itself (encryption) is the most viable option (Enterprise Best Practices, page 33). Encryption, however, is not impregnable, and is even illegal in certain situations. It is currently illegal to transmit encrypted data across United States borders if the encryption key is greater then 40-bit. The reason for this is because the United States government wants to be able to decrypt transmissions

jwagner74@juno.com

across borders to detect criminal activities; the flaw is that if the government can decrypt transmissions, so can criminals. However, since it is law, an e-Commerce organization must comply; therefore, if an e-Commerce organization does business across borders, it must accept such risks. (Ghosh, 1998, page 14)

Supplemental Control Practices: Senior management and auditors should consider the following supplemental control practices over the security of data transmitted over an external network (such as the Internet):

TS.1 - When feasible, the organization should transmit data across controlled paths. (This option is the ideal, but is rarely feasible.)

TS.2 - The organization should chose strong encryption (when not prohibited by law); the encryption used should provide for the protection of the data, the authentication of the sender, and trust in business relationships.

TS.3 - The organization should ensure that any encryption used within the e-Commerce process complies with laws, to avoid legal consequences.

TS.4 - When serving customers or constituents outside the United States, the organization should consider a different data protection process than the one used for customers or constituents within the United States; as to comply with laws, yet maintain a high level of security within the country.

TS.5 - There should be a cost-benefit analysis done whenever a decision regarding business outside of the United States arises. Since there is a greater risk of unauthorized destruction or disclosure of the transmission, a means of determining whether the benefits are worth the risk is essential in decision making.

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION LI – Laws and Investigations

Audit Concern: There should be a means to ensure that an e-Commerce process complies with laws, that potential illegal activities are investigated, and that the organization is prepared to handle any lawsuits which may be incurred.

Organizational Control: Medium.

- Senior management can assign a lawyer or personnel with legal expertise to audit and security staff involved in an e-Commerce presence.
- There are existing laws which give organizations some protection against cybercrime.
- The organization has little influence over laws that are passed in regards to cybercrime, informational property, or encryption.
- All laws, regardless of whether they help or harm, must be complied with.
- It is difficult to remain aware of differences in laws, regulations, and taxation across international, state, county, city, and municipality borders.
- The organization can collect information and assign responsibility for investigation of potential criminal activities to a computer forensics function.
- Once turned over to the authorities, an organization loses control over a legal situation, and loses control over the publicity potential generated.

Risk Assessment: Medium.

- Laws can both protect and harm. For example, laws against cybercrime protect, and laws against strong encryption harm by legally requiring a security exposure (i.e. poorly encrypted communications easily decrypted).
- Lawsuits are costly, can hinder business, and can damage reputation (even frivolous lawsuits).

jwagner74@juno.com

- Laws and investigation options may vary in different locations.
- Pursuing legal action against cyber criminals is difficult, as the organization has limited authority over networks they do not control.
- Contacting the authorities causes the organization to lose control over a situation, and can lead to negative publicity risking reputation (see also Chapter 4, Section PC – Process Continuity).

Existing Standards: Inadequate.

- CobiT DS.8 (Ensure Compliance with External Requirements) addresses compliance with laws and regulations, in limited detail.
- Enterprise Best Practices (Deloitte & Touche) states that it is not enough to be security, but users must known that an e-Commerce process is secure. This can be related to Laws and Investigations: when there is a potential lawsuit or investigation of crime, users should be assured that they can have confidence in using the e-Commerce service. (See also Appendix 3)

As e-Commerce increases the scope of a business process, it can no longer be restricted to one jurisdiction. Additionally, laws are likely to change as e-Commerce becomes more popular. Tax rates may change, and even vary in states and districts. Additionally, in response to the September 11, 2001 attacks, the government is considering further laws and monitoring of Internet transmissions, which could most definitely impact the e-Commerce process. As illegal activities may occur in areas where the organization has no control, coupled with the potential for crime to occur in multiple jurisdictions, investigating incidents is increasingly complex.

Supplemental Control Practices: Senior management and auditors should consider the following supplemental control practices over laws and investigations:

LI.1 - Consider having lawyers or legal experts in an established independent audit function.

LI.2 - Organizational legal counsel should have the authority to be involved in the assurance of an e-Commerce presence.

LI.3 - A computer forensics function should be established, with the authority to investigate potential malicious and/or criminal activity. (Network Security Conference, 2001)

LI.4 - Electronic Commerce processes should collect as much information as

jwagner74@juno.com

possible, to provide evidence for investigation in the event of potential crime.

LI.5 - Organizational policies should clearly state who has the authority to escalate an incident to the level of a suspected crime.

LI.6 - Organizational policies should clearly state who has the authority to notify law enforcement. (Network Security Conference, 2001)

LI.7 - Reputation risk should be considered before authorities are notified of a suspected crime. (see also Chapter 4, Section PC – Process Continuity)

jwagner74@juno.com

CHAPTER 4 – RESULTS

SECTION VE – Virtual Ethics

Audit Concern: As an e-Commerce relationship and information technology provide an organization with enormous capabilities to collect, store, and track information about users, control should be in place to ensure that the rights, privacy, and concerns of users and customers are considered.

Organizational Control: High.

- The organization has complete control over how it uses the information it collect about its users and customers.
- The organization has complete control over policies and privacy statements it generates and makes available to users.

Risk Assessment: Medium.

- The organization must track information about users and customers to ensure authenticity, and to facilitate the investigation of potentially malicious and/or criminal activity (see also Chapter 4, Section LI – Laws and Investigations).
- The benefits of tracking users buying and browsing habits to gain a competitive advantage is high; however, misuse of such information and a disrespect for the privacy of customers can result in a reputation disaster. (See also Chapter 4, Section PC – Process Continuity)
- As the General Accounting Office (GAO) has investigated information tracking practices (through the use of cookies and web logs), and as some states (such as Illinois) are doing the same, laws governing such practices are likely.

Existing Standards: Inadequate.

- COSO addresses “doing the right thing” when dealing with customers. Clearly, respect for the privacy of users and customers fall under this category.

jwagner74@juno.com

A major theme in COSO training I have attended is "doing the right thing when dealing with customers." Often, doing the right thing costs a lot. However, not doing the right thing can cost more in the long term. With Internet communications, and e-Commerce, comes the potential to obtain, use, and even misuse a great deal of information about customers. There may even be laws in this area soon; for example, the GAO audited the information collecting practices of federal agencies (such as the use of cookies and web logs), and the Illinois General Assembly mandated a similar audit of state agencies. With or without laws, however, an e-Commerce organization must carefully examine what information about users should (and should not) be collected, and must be careful about how such information is used. The misuse of information tracking capabilities to gain a competitive advantage can backfire, which could devastate reputation.

Supplemental Control Practices: Senior management and auditors should consider the following supplemental control practices over the ethical control of a virtual process:

VE.1 - Information collected about customers or visitors to the organizations web site should never be shared with external entities without the approval of the customers.

VE.2 - Policies should be made available to customers and web visitors stating what information is being gathered, the means by which it is gathered (i.e. cookies, web logs, etc.), disclosure of how long it will be retained, and assurance that the information will not be shared without permission.

VE.3 - Legal counsel should be involved in decisions regarding information tracking practices, to ensure compliance with laws.

VE.4 - Organizations should be aware of information tracking by third party software used on their web sites and in their e-Commerce processes, and ensure the practices are in line with the organization’s policies. (Some third party software utilizes cookies or web logs; organizations need to be aware of this).

VE.5 - Information should not be gathered unless a justifiable need to so do is demonstrated (it is necessary for e-Commerce transactions, necessary to facility investigation, etc.).

VE.6 - Information collected about users should be adequately secured and protected.

jwagner74@juno.com

CHAPTER FIVE – CONCLUSIONS AND SUMMARY

The results of this project were significantly different than what I expected. I had anticipated identifying several domains of control areas unique to Electronic Commerce. Instead, I found that the same issues that have been dealt with in network, data, and application security are still the issues that need to be addressed in e-Commerce security. The difference lies in this: When applying controls to an e-Commerce presence, however, these same issues are broader in scope, entail increased risk, and those responsible for the security of the e-Commerce presence have less control.

I probably should not have been as surprised by this as I was. Back in Chapter 1, before I even began working on the project itself, I stated the primary reason for this--control *objectives* are normally independent of technology. It is the control *process* (the controls used to fulfill control objectives) that change with technology. For example, in the results, I discussed data transmission security, encryption, and Public Key Infrastructure (PKI); the secure transmission of information is a control objective, encryption is a control process (used to achieve the objective of securely transmitting data), and PKI is a specific technology used in the control process. I addressed PKI, as it is currently a very reliable means of security data. However, I avoided technology (to the extent possible) when developing the Supplemental Control Practices, as the reliability of a technology-specific solution my change; for

jwagner74@juno.com

example, 40-bit encryption used to be a feasible solution, until increased processing capabilities made it easy to crack—PKI may not live forever either. For this reason, and as I desire that the results of this project be valid for a long time, technology-specific areas had to be avoided when possible. However, with the increase scope and risk of e-Commerce security, along with the decreased control, current applicable standards needed to be more specific.

Control Domains not Addressed

The control domains I addressed are clearly not exhaustive. There were other areas I considered, yet did not include. There are three predominant reasons for this: 1) they were not critical, 2) they were adequately addressed by current standards, or 3) time constraints. Here are some examples of control domains I considered, and my justification for not including them:

- Business-to-Business Users Securing B2B users is not as complex as securing B2C users, and an organization has more control because there is a lessened need to satisfy users, and an increased ability to enforce security through contracts (such as third party agreements). With current standards addressing internal users, and section BC providing supplemental control practices for B2C users, this domain would have been redundant.

- External Networks As the organization has little control over external networks, their control lies in protecting the data. This is addressed in section TS, and would have been redundant.

- Public Key Infrastructure (PKI) This area is technology specific, and also discussed in section TS. Deloitte & Touche published "e-Commerce Security - Good Practices for Security Communications" which addresses PKI sufficiently. A PKI domain would add no value to this project, and I

avoided recommending technology-specific solutions.

- Digital Signatures Authentication is covered in sections BC and TS. As with PKI, I avoided technology specific solutions.

- Multi-Tiered Authentication - Other publications, such as the Deloitte & Touche e-Commerce Security series, address this issue. Additionally, authentication beyond a password when attracting customers is not a feasible solution (due to costs and inconvenience to the customer).

- Audit Documentation and Reporting This does not change with e-Commerce. Current standards, particularly CobiT and COSO, are more than adequate in their specifications for evidence and competence, as well as for reporting findings. (see also Appendix 1 and Appendix 2)

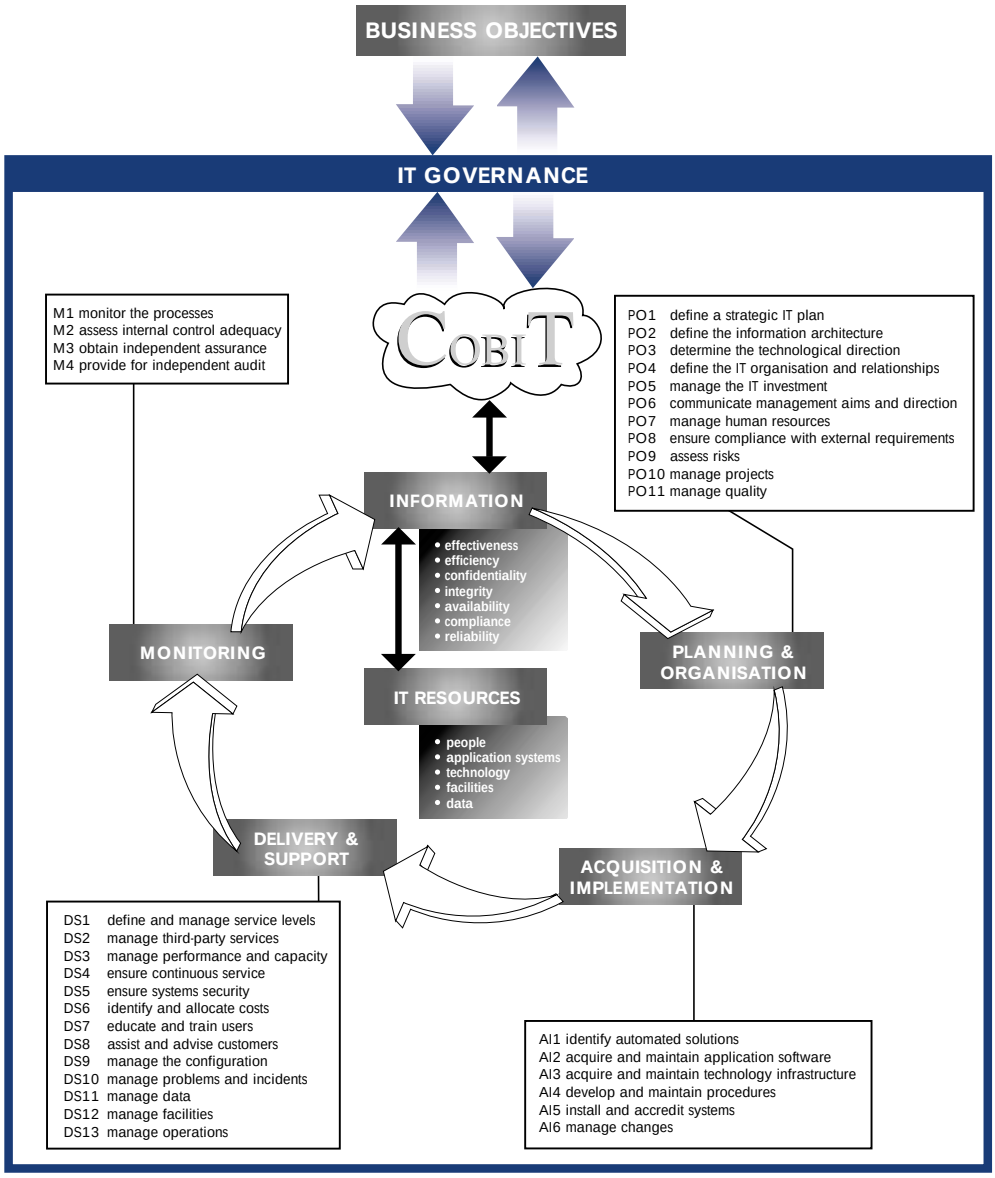
- Virus Control Current standards are more than adequate.

Conclusion

Overall, I am very pleased with the results of my project, and I believe what I have presented adds value to securing and auditing e-Commerce. As previously stated, the results are not what was anticipated. A great deal of the results would be valuable considerations to secure information systems which do not utilized e-Commerce as well. Additionally, the results are not only of value to auditors, but to security administrators and management as well. I believe that the 54 Supplemental Control Practices I have developed are a useful compliment to existing standards, and to the 22 Enterprise Best Practices developed by Deloitte & Touche and published by the Information Systems Audit and Control Foundation.

jwagner74@juno.com

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



BOEING'S PLAN FOR INTEGRATING COSO[1]

In much the same way that our team evaluates the controls of our clients, we've used the following chart as a tool for training and guiding our audit staff in COSO-based audits. For each step, we've noted the control component addressed by the particular steps. Covering the full range of controls-from control environment to monitoring-is the key to successful COSO integration		CONTROL ENVIRONMENT	RISK ASSESSMENT	CONTROL OF ACTIVITIES	INFORMATION & COMMUNICATION	MONITORING
RESPONSIBILITIES AND PLANNING TASKS						
GENERAL AUDITOR	Assign responsibility for COSO integration to team of "subject matter experts."	●				
	Establish expectations for internal audit management and staff to fully support COSO integration.	●				
	Regularly enforce top-level support through memos and staff meetings.				●	
AUDIT MANAGEMENT	Project managers ensure proper implementation of instructions in each audit.			●		
	Audit directors selectively review audit work for compliance with COSO guidance.					●
	Audit directors periodically summarize status of internal control system by business segment.				●	
TEAM OF SUBJECT MATTER EXPERTS	Identify the risks to achieving objectives and define mitigating actions.		●			
	Issue written instructions: Strengthen internal control policy alignment with COSO Publish COSO guidance paper Update internal audit manual to reflect new requirements			●		
	Communicate instructions to internal auditors Introduce concepts at all-hands meeting Conduct four-hour workshops with real-life examples Assign "subject matter experts" to answer questions Identify additional training needs based on peer reviews				●	
	Identify appropriate changes to audit committee reports.				●	
	Conduct internal peer reviews of implementations.					●

RISK ASSESSMENT		
OBJECTIVE	RISKS	MITIGATING ACTIONS
Complete, Consistent Implementation.	Auditors not convinced of priority.	Provide on-going, top-level support.
	Auditors do not perceive credible use of control evaluation information.	Modify audit committee reports to feature control evaluation information.
	Quality declines after initial training.	Write formal instructions; provide follow up training.
	Implementation problems not detected.	Monitor implementation

[1] Dennis Applegate and Ted Willis *Struggling to Incorporate the COSO Recommendations Into Your Audit Process?* (The Institute of Internal Auditors, 1999)

jwagner74@juno.com

e-Commerce Security – Enterprise Best Practices

Developed by Deloite & Touche[1]

There should be a set of security mechanisms and procedures which, taken together, constitute a security architecture for e-Commerce.

There should be measures in place to ensure the choice of the correct protocols for the application and the environment, as well as the proper use and exploitation of their features and compensation for their limitations.

There should be a mechanism in place to mediate between the public network (the Internet) and an organization's private network.

There should be a means to communicate across the Internet in a secure manner.

There should be a process whereby participants in an e-Commerce transaction can be uniquely and positively identified.

There should be a mechanism by which the initiator of an e-Commerce transaction can be uniquely associated with it.

There should be an infrastructure to manage and control public key pairs and their corresponding certificates.

There should be procedures in place to control changes to an e-Commerce presence.

e-Commerce applications should maintain logs of their use, which should be monitored by responsible personnel.

There should be methods and procedures to recognize security breaches when they occur.

There should be features in e-Commerce applications to reconstruct the activity performed by the application.

There should be a means to maintain a provable association between an e-Commerce transaction and the person who entered it.

---

[1] Deloitte & Touche, *e-Commerce Security-Enterprise Best Practices* (Rolling Meadows, Illinois: Information Systems Audit and Control Foundation, 2001)

There should be a means to ensure the confidentiality of data communicated between customers and vendors.

There should be mechanisms to protect e-Commerce presences and their supporting private networks from computer viruses and to prevent them from propagating viruses to customers and vendors.

There should be protection over the devices used to access the Internet.

There should be features within the e-Commerce architecture to keep all components from failing and to repair themselves if they should fail.

There should be a plan and procedures to continue e-Commerce activities in the event of an extended outage of required resources for normal processing.

There should be commonly understood set of practices and procedures to define management's intentions for the security of e-Commerce.

There should be measures in place to prevent information about customers from being disclosed and not used for purposes other than that for which it was obtained, without the customer's permission.

There should be shared responsibility within an organization for e-Commerce security.

There should be communication from vendors to customers about the level of security in an e-Commerce presence.

There should be a regular program of audit and assessment of the security of e-Commerce environments and applications to provide assurance that controls are present and effective.

jwagner74@juno.com

Exposure/Impact Coefficient

Developed by James W. Meritt, CISSP[1]

These values were derived using the combined experience and skills of a number of experts in the arena of information systems security. They are suggested values and do not take the local threat environment or existing countermeasure effectiveness into account.

Network/telecommunications: Modems

For threat:

Power loss:	0.20
Communication Loss:	0.40
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.20
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Network/telecommunications: Routers

For threat:

Power loss:	0.40
Communication Loss:	0.50
Data Integrity Loss:	0.10
Accidental Errors:	0.10
Computer Virus:	0.10
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00

[1] James W. Merrit, *A Method for Quantitative Risk Analysis* (http://www.auditnet.org, 1999)

Destruction of Data:	0.10
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Network/telecommunications: Cabling

For threat:

Power loss:	0.10
Communication Loss 0.10	
Data Integrity Loss:	0.00
Accidental Errors:	0.30
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.50
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.50
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.50
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Network/telecommunications: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.20
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.10

Fire:	0.30
Earthquake:	0.30

Software: Operating System

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.80
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.60
Non-disaster downtime:	0.05
Fire:	0.30
Earthquake:	0.30

Software: Applications

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.40
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.30
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.60
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Software: Other

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.20
Abuse of Access Privileges by Employees:	0.20
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Equipment: Monitors

For threat:

Power loss:	0.00
Communication Loss:	0.00
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.00
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.00
Fire:	0.30
Earthquake:	0.30

Equipment: Computers

For threat:

Power loss:	0.20

Communication Loss:	0.20
Data Integrity Loss:	0.00
Accidental Errors:	0.70
Computer Virus:	0.50
Abuse of Access Privileges by Employees:	0.40
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.20
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.80
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Equipment: Printers

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.05
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.15
Non-disaster downtime:	0.05
Fire:	0.30
Earthquake:	0.30

Equipment: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.20
Computer Virus:	0.30

Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	1.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/information: System

For threat:

Power loss:	0.20
Communication Loss:	0.06
Data Integrity Loss:	0.97
Accidental Errors:	0.50
Computer Virus:	0.95
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	0.02
Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.70
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/Information: Business

For threat:

Power loss:	0.10
Communication Loss:	0.30
Data Integrity Loss:	0.70
Accidental Errors:	0.50
Computer Virus:	0.30
Abuse of Access Privileges by Employees:	0.50
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.30
Theft or Destruction of Computing Resource:	0.40

Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	. 1.00
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Data/Information: Other

For threat:

Power loss:	0.20
Communication Loss:	0.10
Data Integrity Loss:	0.70
Accidental Errors:	0.50
Computer Virus:	0.60
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	1.00
Theft or Destruction of Computing Resource:	0.30
Destruction of Data:	1.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.80
Non-disaster downtime:	0.20
Fire:	0.30
Earthquake:	0.30

Other: Facilities

For threat:

Power loss:	0.20
Communication Loss:	0.00
Data Integrity Loss:	0.00
Accidental Errors:	0.50
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.10
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.10

Fire:	0.30
Earthquake:	0.30

Other: Supplies

For threat:

Power loss:	0.00
Communication Loss:	0.05
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.08
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.07
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.20
Non-disaster downtime:	0.00
Fire:	0.30
Earthquake:	0.30

Other: Documentation

For threat:

Power loss:	0.00
Communication Loss:	0.50
Data Integrity Loss:	0.00
Accidental Errors:	0.11
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.10
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	0.20
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.00
Successful Unauthorized System Access by Outsider:	0.10
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

Other: Personnel:

APPENDIX FOUR

For threat:

Power loss:	0.10
Communication Loss:	0.10
Data Integrity Loss:	0.00
Accidental Errors:	0.10
Computer Virus:	0.00
Abuse of Access Privileges by Employees:	0.30
Natural disasters:	0.50
Attempted Unauthorized System Access by Outsider:	0.00
Theft or Destruction of Computing Resource:	0.00
Destruction of Data:	0.00
Abuse of Access Privileges by Other Authorized User:	0.30
Successful Unauthorized System Access by Outsider:	0.30
Non-disaster downtime:	0.10
Fire:	0.30
Earthquake:	0.30

jwagner74@juno.com

APPENDIX FIVE

Ten Steps to Success in Electronic Commerce[1]

1. Think about the meaning of Electronic Commerce.

Many individuals have found that establishing a common understanding of the term Electronic Commerce is extremely useful. This is not as simple as it sounds because the traditional definition of commerce—the exchange of goods or services, especially among people in one area—is firmly embedded as a paradigm in our minds.

Reexamine this definition outside of the box, and allow for the processing of an exchange of goods and services to take place entirely electronically, and on a global basis. This is in essence the heart and sole of Electronic Commerce.

2. Assess the impact of Electronic Commerce on your business.

Engaging in Electronic Commerce requires rethinking the very nature of the buyer/seller relationship. It requires the fundamental transformation of business because all or most human interaction and paper-based processes within the value chain will need to be changed.

This shift will materially change the way business is conducted, how business is conducted as well as where and when. Electronic Commerce is also destined to alter the long established "view of the marketplace," and the players within that

[1] Albert J. Marcella Jr, Larry Stone, and William J. Sampias, *Electronic Commerce: Control Issues for Securing Virtual Enterprises* (Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation, 1998)

marketplace. In doing so, Electronic Commerce will also have major a major impact on inter- and intra-industry competition and the way business is eventually conducted.

3. Change telecommunications and information technology from a cost center to a strategic enabler.

Viewing technology as a cost center is another old paradigm that has to go. Clearly technology can be leveraged to gain a competitive advantage. It is a bridge to the future, a strategic enabler without which Electronic Commerce simply would not be possible.

Significant investment into the current technological delivery systems are warranted. However, emerging technologies will present your organization with the best position to gain both a strategic and competitive advantage, as these technologies are interwoven into your organizations long-term Electronic Commerce strategy. Integrating technologies such as frame relay processing, digital subscriber lines, ISDN, user of 56K modems, web cast programming, and artificial intelligence (for examples) into the design of Electronic Commerce deliverable services, will create a profound competitive advantage.

4. Use technology to rethink your business.

Don't think in terms of implementing new systems for inventory control or management reports. Think about how to enhance customer services and customer

retention. Rethinking the business is critical for developing a strong, strategic pathway that is technology enabled.

Some of the technologies that will support full blown Electronic Commerce have yet to be conceived, and some are still in the pre-concept stage. This, however, should not stop your organization from thinking outside-of-the-box, and questioning exactly how the organization will be conducting business in the next 3 years. With personal technology-agents on the horizon, push and pull information-content delivery systems knocking at the door, cybernotaries (who certify Electronic Commerce transactions) waiting in the wings, the time is NOW to examine the various emerging technologies and identify those technologies that will provide your organization with a value-added, competitive edge in this evolving hyper-commerce environment.

5. Balance technology with people.

Integrating people into the new process is vital, especially in the transitional phase. The introduction of electronics into the process must provide significant additional value for the approach to be successful.

Ensure that the evolution of your organization's Electronic Commerce strategy and eventual Electronic Commerce delivery system itself provides for the interaction of the end-user, and that appropriate feedback and control mechanisms are designed into the final overall EC environment.

6. Create a transitional strategy or iterative steps.

Smart organizations are using their technological lead for short- and long-term strategic benefit.

Do not assess your organizations strengths (or weaknesses) in terms of today's technologies, but envision what technologies will be available three years from now, and how those technologies will be incorporated into your organization's business delivery systems, as value added benefits. Develop a multi-tiered implementation plan that draws upon existing technology yet allows for the migration to newer technologies as they become available. Seek alternative solutions and partnerships, reinventing the way your business is conducted, to compete and survive in the Electronic Commerce marketplace, and how your customers are reached and serviced, will be the difference between organizations who fail and those that survive.

7. Remember that technology can raise some barriers.

The same technologies that provide such overwhelming promise of profitability and competitive advantage also raise serious barriers to widespread deployment and proliferation.

Before launching head long into Electronic Commerce, part of the firm's implementation strategy should be an examination of the potential impediments to a successful Electronic Commerce initiative. Eventual changes in commerce laws, business practices, trading partner relationships, information collection and

distribution methods, and emerging technologies in general, dictate that a firm established a solid plan to address these changes, determine their potential impact upon the firm's ability to successfully reach its Electronic Commerce goals, and craft solutions that will allow the firm to breech these potentially threatening barriers.

8. First focus on the overall goal.

Do not get sidetracked by secondary issues such as human resources, security, or capacity planning. Assign smaller task forces to address these issues, but keep focused on the long-range goal.

It is important to address security and control considerations in the design of any new application (such as Electronic Commerce). These issues should not, however, impede the successful completion of the Electronic Commerce initiative. Concerns such as the ability to audit the Electronic Commerce infrastructure, control access, track orders, payments, etc., should be addressed throughout the design of the Electronic Commerce platform. The overall focus of a competitive Electronic Commerce system should be value-added provided to the end-user. Yet, this should not sacrifice good internal control systems and methods.

9. Educate senior management.

Take proactive action to expose your organization's senior management to the technologies at hand, and demonstrate the impact of Electronic Commerce by

showing them examples of competitor's net sites, which are already operational, and which may already be attracting your customers.

There is no better justification than a picture is worth a thousand words. Viewing a competitor's Electronic Commerce site in operation, and examining the potential impact on revenues, may do more than convince senior management of the necessity of committing to an aggressive Electronic Commerce strategy, than any amount of analysis, report writing or politicking could ever achieve.

10. Get started - now!

Your firm's competitors and business partners are already moving ahead (simply browse the Internet and see for yourself). Become proactive and get senior management moving. Begin with a simple web page and then expand into implementing your entire Electronic Commerce business strategy.

Overall, bottom line, as Nike encourages all—Just Do It!!!

> *"The play it safe reaction doesn't work anymore. If you play it safe, you'll die. If you don't innovate, you are taking a risk."*
>
> *-Erick Brethenoux, analyst for the Gartner Group, Inc., Paris*

APPENDIX SIX

Electronic Commerce Glossary[1]

Acceptance Testing (AT): The testing performed by a user to determine that an automated system (equipment or software) for a specific task or environment, e.g., a translator for a specific application and interchange format, performs according to specification.

Acquisition Manager (AM): The system/equipment program manager, the program manager's staff, and other DoD officials responsible for determining contract requirements for the generation, acquisition, and use of defense system/equipment data, and having acquisition authority for defense systems and equipment.

Ada: A computer language designed as a standard for U.S. government and NATO procurements. Ada is a required language for mission-critical projects.

ANSI (American National Standards Institute): The American National Standards Institute (ANSI) is a privately funded, non-profit organization which coordinates the development of voluntary standards in the United States and is the agency that approves standards (as American National Standards). It coordinates and manages U.S. participation in the work of several non-governmental international standards organizations, including ISO and IEC (NCGA). ANSI's membership consists of over 1000 companies and organizations.

Analog: Continuously variable. Until recently almost all audio signals were analog. At any instant, it could have a value between zero and a few volts and could be graphed as a flowing waveform. In contrast, at any instant, a **digital** signal can have the values of 0 or 1.

ANSI X12: The ANSI X12 standards specify the format and data content of electronic business transactions.

Applet: A miniature application - an enhancement to a web page involving the embedding a foreign type of program in the page.

Application Profile: A number of application protocols required for a specified task or industry sector.

Application Protocol (AP): Defines the context for the use of product data and specifies the use of the standard in that context to satisfy an industrial need. [Associated with STEP] , United States Government. "Military Standard 1840-B" 3 November 1992.

Archie: A system for locating files that are stored on FTP file servers. A search utility. A keyword search service that searches the directory and file titles of all FTP sites that are indexed.

ARPAnet: The name by which the Internet was originally known.

ARPA (Advanced Research Projects Agency): An agency within the defense department that distributes funds for defense related research projects. ARPA (*AKA* DARPA) provided the initial funding for the development of platform independent wide area internetworks. This project eventually became the Internet.

ASCII (American Standard Code for Information Interchange): The American Standard Code for Information Interchange is used extensively in data transmission. The ASCII character set includes 128 upper and lower case letters, numerals and special purpose symbols, each encoded by a unique 7-bit binary number. ASCII text is a subset of the ASCII character set consisting principally of the printable characters.

Attribute: Qualifying property of an HTML tag. Attributes are usually optional.

Backbone: A central high speed network that connects smaller, independent networks. the NSFnet is an example. The connections between the primary computers in a network. Stub networks branch off the backbone.

Bandwidth: Used to express the maximum possible throughput of a data link in **bits per second**. A T1 line has a bandwidth of 1.544 Mbps. A 28.8k baud modem has a nominal bandwidth of 0.0288 Mbps.

Bar Coding: Graphical representation (generally narrow and wide bars) that represent one of a number of numeric or alphanumeric standards.

---

[1] Definitions provided by Precision Measurement Equipment Laboratories (http://www.pmel.org/EC-Glossary.htm)

jwagner74@juno.com

APPENDIX SIX

Baud: A measurement of signaling speed of a data transmission device Baud rate does not equal bits per second.

BPR (Business Process Re-engineering: The fundamental analysis and radical redesign of everything: business processes and management systems, job definitions, organizational structures and beliefs and behaviors to achieve dramatic performance improvements to meet contemporary requirements. Information technology (IT) is a key enabler in this process.

Browser: A World Wide Web client. *See web browser*

Bulletin Board Service (BBS): A bulletin board is similar to a network and thus Internet. Requirements for a bulletin board are a computer, modem, and preferably bulletin board software. A bulletin board can contain directories of files (for user downloading) and e-mail facilities (where users can exchange/or post messages). Based on their access privileges, those using a bulletin board can read, download (copy from the bulletin board), upload (place on the bulletin board), and even modify stored files. Bulletin boards can be on the Internet. Bulletin board software is required to allow the bulletin board owner to place limits on access. (i.e., not all BBS users should be allowed to modify files that are stored on the BBS. Not all of the BBS's users would be allowed full access to the computer on which the BBS is stored.

Cache: Cache memory is a small area of very fast RAM used to speed exchange of data.

CAD (Computer-Aided Design): The application of information technology to elements of the design process for manufactured, assembled, and constructed products, covering both drafting applications (in the creation, modification, storage, and production of engineering and other technical drawings) and modeling (the generation and use of full three-dimensional models).

CAE (Computer-Aided Engineering): The application of information technology to elements of the design and engineering process. It includes all types of performance systems, e.g., heat transfer, structural, electromagnetic, aeronautics, and acoustic analysis.

CALS (Continuous Acquisition and Life-cycle Support): *(formerly Computer-Aided Acquisition and Logistic Support):* CALS is a global strategy to further enterprise integration through the streamlining of business processes and the application of standards and technologies for the development, management, exchange, and use of business and technical information.

CALS Test Network (CTN): The CALS Test Network (CTN) is a confederation of hundreds of industry and government organizations that have agreed to evaluate and demonstrate the interchange and functional use of digital technical information using CALS standards. This is accomplished through a collaborative multi-service effort.

CAM (Computer-Aided Manufacturing): The application of information technology to the control and management of manufacturing processes, normally restricted to the control of machine tools such as lathes and mills, where the tool is directly controlled by a computer.

CASE (Computer-Aided Software Engineering): CASE is an umbrella term for a collection of tools and techniques which are said by their distributors to promise revolutionary gains in analyst and programmer productivity. The two prominent delivered technologies are application generators and PC-based workstations that provide graphics-oriented automation of the front end of the development process.

CBT (Computer-Based Training): Training which is delivered via a computer. Computer-based training includes tutorials, drill and practice, simulations, testing and may also include embedded training. Computer-based training programs are already delivered in digital form to the government.

CCITT Group 4): This CALS standard for raster graphics incorporates tiling, which divides a large image into smaller tiles. Graphic files are exchanged in CCITT/4 format in a compressed state so they take up much less file space.

CCITT: Consultative Committee for International Telephone and Telegraphy International committee that specifies international communication standards.

CD ROM, CD ROM Drive (*Compact Disk Read-Only Memory***):** A read-only disk storage technology that provides up to 600Mb of space in about the same space as a 3.25 in. computer diskette (which stores 1.44Mb). Data stored in this format cannot be modified or updated. An additional CD (computer disk or compact disk) ROM drive is required to access and use data stored in this format and the data cannot be changed or updated. Access speeds are slower than from a standard computer disk drive. The CD ROM drives will typically access both computer disk and compact disk music formats. CD ROMs use a laser technology while standard computer diskettes use a magnetic technology. Neither technology has reached its limits in terms of storage capacity or access speed.

APPENDIX SIX

CE (Concurrent Engineering): A systematic approach to creating a product design that considers all elements of the product life cycle from conception of the design to disposal of the product, and in so doing defines the product, its manufacturing processes, and all other required life cycle processes such as logistic support.

CGI, cgi-bin (Common Gateway Interface): The CGI through which binary files and HTML files communicate. CGI is not a computer language. CGI scripts are commonly written in PERL (or AppleScript) and run in the background on the web server. CGI is the mechanism that has become a standard way of extending the capabilities of a web server. The counter seen on this and other home pages is typically done in a CGI. When you fill out a form, CGI was the likely recipient of the data that was sent back and send it on to a database system. API (Application Program Interface) is a higher performance alternative to CGI. With support from both Netscape and Microsoft, these serve extensions offer opportunities for web publishers to create more sophisticated (and useful) sites.

Client Pull: A simple type of Web animation in which a series of pages is loaded in succession, governed by concealed coding in the headers of the HTML file.

Clipboard: A part of computer memory used as temporary storage for anything cut (Ctrl-X) or copied (Ctrl-X) to it. Text and images stored on the *clipboard* can be pasted (Ctrl-V) into another part of the document or in another document. New items are copied over (i.e. replace) what was previously on the clipboard

CGM (Computer Graphics Metafile): This file format standard is a two-dimensional picture description or vector-oriented illustration data delivered in digital format. CGM is suited for illustrations often found in training, maintenance, and technical manuals.

CIM (Computer-Integrated Manufacturing): The application of information technology to the management of complete systems or subsystems within a manufacturing environment, characterized by the integration of many separate applications such as CAD, CAM, CAE, and robotics together with commercial applications such as stock control, spares ordering, and process planning.

CIM (Corporate Information Management): The US Department of Defense initiative to streamline and improve the way information is managed throughout the military. The Information Management philosophy is founded on business process improvement.

CITIS (Contractor Integrated Technical Information Service): A technical information service based on the integration of databases (contractor , subcontractor, and government) contractually established and managed by the defense contractor to receive, maintain, and provide access to technical and support information on a defense system.

Client: A computer or software that requests a service of another computer system or process (a "server"). For example, a workstation requesting the contents of a file from a file server is a client of the file server.

CMS (Life-cycle Management System): A set of processes (which may include computer-aided software engineering tools) which facilitate the creation, tailoring, and navigation of a system development life cycle. A life cycle management system may take the form of an integrated project support environment or an estimating system linked to a project scheduling and tracking system.

COCOMO: A tool for manpower estimating, life cycle costing, and scheduling tool for manpower estimating, life cycle costing, and scheduling. * National Security Industrial Association. "CALS Expo '93, Proceedings and Reference".

Communication (COM) port: Logical designation of serial communication channels.

Communication Protocol (CP): The rules governing the exchange of information between devices on a data link. * Fairfax CALS Shared Resource Center, 1994.

Compliance: The act or process of complying to a desire, demand, or proposal. * Adapted from: Sharon

Component Testing (CT): Is conducted to verify the implementation of the design for one software element (e.g., unit, module) or a collection of software elements. * Sharon J. Kemmerer. Department of Commerce, United States Government. "CALS Testing Programs, Status and Strategy" October 1992.

Configuration Management (CM): CM controls and manages product description with its supporting technical and scientific information. * Fairfax CALS Shared Resource Center, 1994.

Conformance Testing (CT): The testing of a candidate product for the existence of characteristics required by a standard. Its primary activity is to ensure specified behavior of implementations. Additional benefits include: clarifying the standard for guiding future implementation, producing a feedback loop to the standards making bodies for

improvements to the standard, encouraging commercial development by supporting a baseline for commonality in all products, and providing greater confidence on the part of the potential enterprise user. Conformance-tested implementations increase the probability these same implementations will be able to inter-operate, but provides no guarantee.

COTS (Commercial Off The Shelf): Commercial Off The Shelf refers to software and hardware technology which is commercially available and requires minimum changes (design/development), if any, before implementation.

Cyberspace: A term coined by Wm. Gibson in *Necromancer* to describe the sum total of computer accessible information in the world.

Database Management System (DBMS): Software designed to manipulate the information in a database. It can create, sort, display selected information, search for specific information, and perform many other tasks of a database. This kind of software allows speed of access and the ability to automatically produce reports.

Data Dictionary (DD): A repository of information about data, such as its meaning, relationships to other data, origin, usage and format. The dictionary assists company management, database administrators, systems analysts and application programmers in effectively planning, controlling and evaluating the collection, storage and use of data. A data dictionary manages data categories such as alias, data elements, data records, data structure, data store, data models, data flows, data relationships, processes, functions, dynamics, size, frequency, resource consumption and other user-defined attributes.

Data Management Standards: Data management standards will provide common definitions of the data elements, their attributes, relationships, data integrity constraints, and database access rules. This includes standards for system and data protection and security.

Data Model: The logical data structure developed during the logical database design process is a data model or entity model. It is also a description of the structural properties that define all entries represented in a database and all the relationships that exist among them.

Data Modeling: A structured method for representing and describing the data used in a business function automated system. Data modeling is used in combination with two other structured methods, data flow analysis and functional decomposition, to define the high-level structure of business and information systems. Its primary function is to define the attributes of and relationships among data items.

Declaration File: A file accompanying any set of transferred files comprising a document; provides all information necessary to the successful disposition of the digital files at the destination, but has no purpose beyond that function.

Defacto Standard (Proprietary Standard): A standard which has been endorsed by industry or government, but not officially approved by an accredited standards body such as ISO.

Descriptive Markup: Markup that describes the structure and other attributes of a document in a non-system-specific manner, independently of any processing that may be performed on it. In particular, it uses tags to express the element structure.

Destination System: The computer hardware, software, and network receiving transferred data.

Development Testing: Development testing is equivalent to "proof of principal" as proposed standards are being developed, and before those draft standards achieve technical stability.

DID (Data Item Description): A DID identifies specific data requirements, which may include the format of a report used to display the data. Most current DID's were prepared with only the hard copy (paper, aperture card, etc.) document environment in mind. In a CALS environment, two aspects of data acquisition must be examined to determine whether existing DID's are adequate: the deliverable itself (documents, processable data files, interactive access), and the delivery mode (physical media or telecommunications).

Digital: Characterized by being either on or off with no intermediate value. The term is applied to computer data in transit and contrasted with *analog*.

Digital Technical Data: Includes the part descriptions, product specifications, and standards that the initial designer draws upon; the engineering drawings and product data used in design and manufacturing; the information needed to guide the people who operate the system in the field, or who support and maintain it at all echelons of the logistic support structure; the materials needed to train new operators, maintainers and other technicians; and the information needed for re-procurement, re- manufacturing, modification, and feedback to industry for future design.

APPENDIX SIX

Direct Connection: A hard wired connection between a computer and the Internet giving the computer an **IP address** and the ability to function as a Web site. Contrasted to a dial up connection

Distributed Database: A database whose objects (tables, views, columns and files) reside on more than one system in a network, and can be accessed or updated from any system in the network.

Distributed Systems: Refers to computer systems in multiple locations throughout an organization working in a cooperative fashion, with the system at each location serving the needs of that location but also able to receive information from other systems, and supply information to other systems within the network.

Document: A set of text and/or graphical data organized and formatted for direct human interpretation. A document can be delivered as printed pages or digitally in the form of composed page images.

Document Image File: A digital data file representation of a human interpretable document. Examples are raster image files and page description language files.

Document Type: A class of documents having similar characteristics; for example journal, article, technical manual, or memo.

Document type declaration: A markup declaration that contains the formal specification of a Document Type Definition (DTD).

DTD (Document Type Definition): SGML is a metalanguage used to define particular document types. One could create an SGML for a cookbook that had only five tags. Alternatively, one could use SGML to define a web document and call it HTML. SGML is an International Standard for marking up electronic documents, ISO 8879

Document Type Definition: When you create a new markup language in SGML , you write what is called a DTD which defines what your markup language looks like and how to handle documents that have been written in that markup language. When you use an HTML validator, you are checking the validity of your documents against an HTML DTD. HTML 1.0 and HTML 3.0 comply with the SGML standard. The core SGML philosophy is that documents should be defined based on their content and not on their appearance. This has been a source of conflict because most electronic publishers want to control the appearance of their pages.

Domain Name System (DNS): A scheme for translating numeric Internet addresses into "user friendly" strings of word segments denoting user names and locations. The Internet naming scheme consists of a hierarchical sequence of names, from the most specific to the most general (left to right), separated by dots, for example luorc.ecrc.edu . *(See also: IP address)*

Dot Pitch: Dot pitch is the space between pixels. The smaller the number, the sharper the image will appear. (.28mm is better than .32mm)

Drawing: An engineering document or digital data file(s) that discloses (directly or by reference), by means of graphic or textual presentations, or a combination of both, the physical and functional requirements of an item.

DTD (Document Type Definition): A DTD is the formal definition of the elements, structures, and rules for marking up a given type of SGML document. You can store a DTD at the beginning of the document or externally in a separate file.

Electronic Bulletin Board: A shared file where users can enter information for other users to read or download. Many bulletin boards are set up according to general topics and are accessible throughout a network.

E-Mail (Electronic Mail): Any communications service that permits the electronic transmission and storage of messages and attached/enclosed files.

EC (Electronic Commerce): The end-to-end digital exchange of all information needed to conduct business. Examples include EDI transactions, electronic mail, archives, audit trails, and all forms of records, including graphical images. Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT) and Continuous Acquisition and Life-cycle Support (CALS).

EDI (Electronic Data Interchange): The inter-organizational, computer-to-computer exchange of structured information in a standard, machine-processable format.

EDIF (Electronic Design Interchange Format): A neutral, platform independent format for the interchange of integrated circuit design data from design to manufacturing organizations.

EDIFACT (EDI For Administration, Commerce and Transport): United Nations rules for Electronic Data

Interchange for Administration, Commerce and Transport. They comprise a set of internationally agreed upon standards, directories and guidelines for the electronic interchange of structured data related to trade in goods and services between independent computerized information systems.

EFT (Electronic Funds Transfer): Electronic movement of data between banks which results in a value transfer between accounts.

EFT (Electronic Funds Transfer): EFT is a technology (one of the electronic commerce technologies) that allows the transfer of funds from the bank account of one person or organization to that of another. EFT is also used to refer to the action of using this technology. It is an important addition in the organization that implements EDI in their organization.

Encryption: A method of ensuring data secrecy. The message is coded using a key available only to the sender and the receiver. The coded message is sent to the receiver and then decoded upon receipt.

Engineering Data: Any technical data (whether prepared by the Government, contractor, or vendor) relating to the specification, design, analysis, manufacture, acquisition, test, inspection or maintenance of items or services. Engineering data is comprised of all information that contains authoritative engineering definition or guidance on material, constituent items, equipment or systems practices, engineering methods, and processes.

Enterprise Integration (EI): Is the removal of organizational, process, and informational barriers to the smooth and effective flow of material and products between the activities of an enterprise.

Enterprise: Is a collection of organizations and people formed to create and deliver product to customers.

ERP (Enterprise Resource Planning): ERP represents the next generation of manufacturing resource planning (MRP II) software. ERP's usefulness and power lies beyond the present function boundaries of MRP II. Beyond the standard functionality that is offered, other features are included, e.g., quality process operations management, and regulatory reporting. In addition the base technology used in ERP will give users software and hardware independence as well as an easy upgrade path. Key to ERP is the way in which users can tailor the application.

ESnet (Energy Sciences Network): This is a Department of Energy (DOE) system that provides the full text of select DOE documents. Many of these documents are related to computers and information policy. It also contains gateways to a variety of energy-related sources and downloadable public domain software.

Expert System: A software system with two basic components: a knowledge base and an inference engine. The system mimics an expert's reasoning process.

FAQs (Frequently Asked Questions): A FAQ is a list of frequently asked questions. On the Internet a FAQ may exist as a feature of an interest groups or be a mailing list. Each FAQ addresses a specific topic with a list of questions and their answers.

FCIM (Flexible Computer Integrated Manufacturing): FCIM is the integration of equipment, software, communication, human resources, and business practices within an enterprise to rapidly manufacture, repair, and deliver items on demand with continuous improvements in the processes. The FCIM initiative is a Joint Service and Agency effort to establish and implement the procedures and processes needed to expand the use of flexible manufacturing technology within the Department of Defense. The Joint Logistics Commanders chartered the Joint Technical Coordinating Group on FCIM (JTCG-FCIM) with the mission to coordinate participation of the Service Logistics Commands in the development and implementation of FCIM throughout the DoD.

File Transfer Protocol (FTP): A way of transferring files between computers. A protocol that describes file transfers between a host and a remote computer. It is also used to program based on this protocol.

File: A digital repository of organized information consisting of records, items or arrays, and data elements.

Finger: A software tool used to determine whether another user is logged on to the Internet. It can also be used to find out a user's address.

FIPS (Federal Information Processing Standard): Standards published by the U.S. National Institute of Standards and Technology, after approval by the Dept. of Commerce; used as a guideline for federal procurements.

Firewall: A computer system that sits between the Internet and a company's LAN. It is a means of automatically limiting what a company's computer system will pass along to outside computer systems. It acts as an active gateway to keep non-company entities from accessing company confidential data.

APPENDIX SIX

FOSI (Formatting Output Specification Instance): A FOSI is used for formatting SGML documents. It is a separate file that contains formatting information for each element in a document.

FTAM (File Transfer, Access and Management): The Open Systems Interconnection standard for file transfer (i.e., the communication of an entire file between systems), file access (i.e., the ability to remotely access one or more records in a file) and management (e.g., the ability to create/delete, name/rename a file).

Gateway : Used in different senses (e.g., Mail Gateway, IP Gateway), but most generally, a computer that forwards and routes data between two or more networks of any size. *See CGI.*

Gopher: A search tool that presents information in a hierarchical menu system somewhat like a table of contents.

GOSIP (Government Open Systems Interconnection Profile): The U.S. government's OSI protocols that address communication and inter-operation of computer systems across government agencies; they mandate that network procurements comply with the Open System Interconnection model.

Graphics Standard: A technical standard describing the digital exchange format of graphics data. (CCITT Group 4 and CGM are examples).

GTIS (Government Technical Information Systems): The collection of automated data processing systems and applications used by government agencies and offices to enter, update, manage, retrieve, and distribute technical data from a specific Integrated Weapon System Data Base.

HTML (Hypertext Markup Language): HTML is essentially an SGML DTD for hyperlinked text with in-line graphics which serves as the language of the Internet's World Wide Web. Documents that are formatted with proprietary software are typically too big for efficient transmission. A 4 Kb page in plain text can double in size with the addition of proprietary formatting codes. A mark up language does not have this overhead. Instead of defining precisely how the document should appear, it identifies the important parts of a document, including text that should be emphasized. HTML codes are so compact that they have little or no effect on the file size.

HTTP (Hypertext Transfer Portico): The protocol developed at CERN that enables a browser (or client) to send out a request to a web server via the Internet.

Hypertext : Text that is not limited to a single linear or sequential path through it. Hypertext provides the option of non-sequential, non-hierarchical navigation through a body of information. Ted Nelson envisioned hypertext in 1965. His two books *Computer Lib* and *Dream Machines* are available in one volume from Microsoft press. He defines hypertext as non-sequential writing. Just as there is good and bad sequential writing, there is good and bad hypertext. The point is to organize data in a way that readers can easily pick the chunks they find relevant without following a sequence dictated by the author.

Hyperbolic Space or Hyperspace: In Klien's geometry, a space with manymore dimensions that the four we are used to (height, width, depth, and time) Nelso asked, "What is the hyperspace of a document?" It would be all of the concepts it contained.

ICR (Intelligent Character Recognition): A technology that employs either software only or software and hardware to automatically recognize and translate raster images into structured data.

IDEF0: A functional modeling method for complex manufacturing environment which when graphically represented show the structural relationships between the manufacturing processes.

IDEF1: a graphical method which extends the process model by modeling the information flows and the entity relationships. IDEF1X provides extensions to IDEF1 with different graphical representation.

IEEE (Institute of Electrical and Electronics Engineers): Organization of engineers, scientists and students involved in electrical, electronics, and related fields; also functions as a publishing house and standards-making body.

IETM (Interactive Electronic Technical Manual): An interactive, intelligent access environment for large volumes of graphical and text-based technical information. It provides a complete electronic technical manual that is linked to text, drawings, photographs, [video] and fault isolation procedures.

IGES (Initial Graphics Exchange Standard): A neutral file format for the representation and transfer of product definition data among CAD/CAM systems and application programs.

A picture, graph, diagram or other form of graphical representation contained within a technical publication.

ILS (Integrated Logistics Support): Encompasses the unified management of the technical logistics elements that

plan and develop the support requirements for a system. This can include hardware, software, and the provisioning of training and maintenance resources.

Information Engineering: A methodology for developing an integrated information system based on the sharing of common data, with emphasis on decision-support needs as well as transaction processing requirements. It assumes logical data representations are relatively stable, as opposed to the frequently changing processes that use the data. Therefore, the logical data model, which reflects an organization's rules and policies, should be the basis for systems development.

Information Infrastructure: A structured collection of information system components and organization processes that enable the flow of necessary information to effect enterprise integration.

Information Superhighway: The Information Superhighway is a network that will potentially connect every government agency, business, and citizen providing a means of rapid access to information (in digital form) and electronic communication to every business and citizen in the country. This vision is an unprecedented nationwide (and ultimately worldwide) electronic communications network that will provide just about any sort of electronic communication imaginable. Your computer, interactive TV, telephone, or other technology will enable access. The purpose of the information superhighway is to provide an infrastructure for, among other things, electronic commerce, in a variety of forms including electronic banking, electronic data interchange, inventory managing, taxpaying, video conferencing, medical diagnosing, and virtually any other business activity. The closest approximation to the Information Superhighway at this time is the Internet.

Integration: Can be described as consisting of three main components: physical integration, the connection of the hardware; data integration, the ready exchange of data between applications without loss of functionality; and lastly business integration, the integration of the functions needed to support decisions, monitor and control business.

Intelligent Gateway: Intelligent gateway is a technology which makes the complexities of on-line database connection and authorized interrogation transparent to users. Intelligent gateways provide transparent logos, transfer user prompted queries into that can be read by non-standard database retrieval programs.

Inter-operability Testing: Inter-operability testing addresses the problem of data interchange between two vendor products within a data system, or between two data systems.

Interactive Access: The ability to access authorized portions of the source data maintained in contractor or Government systems via on-line telecommunications data transfers in real or near-real time using various types of queries.

Internet Protocol (IP): A standard that describes how packets of data are transported across the Internet and recognized as an incoming message.

Internet Relay Chat (IRC): A software tool that makes it possible to hold real-time keyboard conversations on-line.

Internet: The series of interconnected networks that includes local area, regional, and national backbone networks. Networks in the Internet use the same telecommunications protocol (TCP/IP) and provide electronic mail, remote login, and file transfer services. The global Internet, the world's largest internet, includes nearly every university, government, and research facility in the world. Since 1994, the number of commercial sites has increased exponentially to the point where, in 1996, 50% of the nodes on the Internet are commercial (.com) sites. The Internet is the closest thing that we have the Information Superhighway. It started with four interconnected computers in 1969 known as ARPAnet.

InterNIC: The official source of information about the Internet. Its goal is to: 1) provide Internet information services, 2) supervise the registration of Internet addresses, and 3) develop and provide databases that serve as white and yellow pages to the Internet.

Intranet: An intranet is a LAN or WAN operating under the TCP/IP and HTTP protocols but, usually for security reasons, is not connected to the global Internet. The information on the intranet is available only to those with network access.

IP Address: The numeric address of a computer connected to the Internet; also called Internet address. See *domain name* and *TCP/IP*.

IP (Internet protocol) : The Internet standard protocol that provides a common layer over dissimilar networks, used to move packets among host computers and through gateways if necessary.

IPDB (Integrated Product Data Base): A common product data base enables changes and modifications available to

users simultaneously.

IRDS (Information Resources Dictionary System): IRDS is a standard, not a system. It specifies services performed by a data administrator in cataloguing, documenting, managing, and using data dictionaries. It is based on the entity-relationship model, and allows attributes on relationships.

IRQ: Interrupt request, used to get the attention of the system to perform a task.

ISDN (Integrated Services Digital Network): The technical standards and design philosophy according to which digital networks will be designed. ISDN provides high-speed, high-bandwidth channels to every subscriber on the network, achieving end-to-end digital functions with standard equipment interface devices. The networks will enable a variety of mixed digital transmission services to be accommodated at a single interface (including voice and circuit and packet switched data).

ISO (International Standards Organization): A voluntary, non-treaty organization established in 1949 to promote international standards.

ISO (International Standards Organization): ISO is the international standards organizations that is similar in function to ANSI. They do not create standards but as with ANSI the provided a means of verifying that a proposed standard has met certain requirements for due process, consensus, and other criteria by those developing the standard. After this verification the standard is approved as an international standards by ISO.

ISO 9000: SO 9000 is a series of international standards that provides quality management guidance and identifies quality system elements that are necessary for quality assurance. In other words, the ISO 9000 series standards have two main roles: to provide guidance for suppliers of all types of products that wish to implement effective quality systems (or improve existing ones); and to provide the generic requirements against which that quality system can be evaluated.

ISO/OSI (International Standards Organization/Open System Interconnection): A standard, modular approach to network design that divides the required set of complex functions into manageable, self- contained, functional layers.

IWSDB (Integrated Weapon Systems Database): A physically distributed, logically linked data structure for the total collection of shared product definition and support data for one or more defense systems.

JCALS (Joint Computer-Aided Acquisition and Logistic Support): The JCALS program is the Department of Defense's lead system for implementation of CALS. The functionality of JCALS will provide automation of technical manuals and other maintenance documents. Fairfax CALS Shared Resource Center, 1994.

JCMO (Joint CALS Management Office): The JCMO was established as a joint (multi) military organization comprised of Army, Navy, Air Force, Marine Corps and Defense Logistics Agency (DLA) in order to implement common (joint) CALS solutions. The JCMO developed the DoD CALS Architecture released in June 1991.

JEDMICS (Joint Engineering Data Management Information and Computer System): The standard DoD program for management of engineering drawings and related technical data. It automates the DoD's engineering data repositories using an integrated suite of off-the-shelf hardware and software. This system enables improved acquisition, storage, update, and retrieval of technical information. Plans call for installation of JEDMICS at 25 sites by Fiscal Year 1995.

JIT (Just-In-Time) Inventory: A method of controlling and reducing direct and work-in-process inventory by having suppliers deliver material "just in time" to manufacturing. **JPEG (Joint Photographic Experts Group):** A widely accepted, international standard for compression of color images.

Kilobit and Kilobyte: A kilobit is 1000 bits. A byte usually equals 8 bits. Thus, a Kilobyte=8000bits. The former is generally used to indicate the speed of transmission (kbps or kb/s). The second along with Mb is typically used to as a measure of storage capacity.

LAN (Local Area Network): A user-owned and operated data transmission facility connecting a number of communicating devices (e.g. computers, terminals, word processors, printers, and mass storage units) within a single building or campus of buildings.

Layer: In the Open System Interconnection reference model, refers to a collection of related network-processing functions that constitute one level of a hierarchy of functions.

LCC (Life-Cycle-Cost): Refers to the total cost of a product over the full life of the product. The cost includes design, development, production, and support.

APPENDIX SIX

LDM (Legacy Data Management): The process of identifying and evaluating historical information and defining potential solutions and requirements for long-term usage of that data in a cost effective manner.

Lead Time: A span of time required to perform an activity. In a production and inventory control context, the activity is normally the procurement of materials or product from either an outside supplier or a company's own manufacturing facility. The individual components of any given lead time can include some or all of the following: order preparation time, queue time, move or transportation time, receiving and inspection time.

Legacy Data: Existing data that has been acquired by an organization.

LOA (Letter Of Agreement): A document executed between two or more parties outlining specific agreements relating to the accomplishment of an action.

Logistics: Logistics is the science of planning and implementing the acquisition and use of the resources necessary to sustain the operation of a system.

LSA (Logistics Support Analysis): A modeling process used to recognize the maintenance, training and the number of people that are required to get the system running and to maintain the system.

LSAR (Logistics Support Analysis Record): That portion of LSA documentation consisting of detailed data pertaining to the identification of logistic support resource requirements of a system or equipment.

Magnetic Tape: Magnetic tape is the preferred physical medium for delivery of technical data in digital form because it is a mature, stable technology that is able to handle the large volumes of data typically involved in a major weapon system acquisition.

Mailing List: A BBS (see the definition of BBS) like server that acts like a giant message router. All messages sent to the mailing list are automatically sent to all members of the mailing list.

Maintainability: The measure of the ability of an item to be retained in or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

MANTECH (Manufacturing Technology): This DoD program may provide a source of viable technology transfer for program specific CALS initiatives. The MANTECH program was established to help develop and improve manufacturing processes, techniques and equipment to provide timely reliable and economical production in DoD.

MAP (Manufacturing Automation Protocol): A largely moribund communication standard proposed by General Motors in 1986 that ideally would have enabled system devices within a manufacturing company to communicate among themselves.

Markup: Tags that are added to the data of a document in order to convey information about it.

MIL-HDBK (Military Handbook): A document published by the Military Defense Department as a guide for implementing various programs.

MIL-HDBK-59 (Military Handbook 59): The "DoD CALS Program Implementation Guide," is not a standard. It provides the acquisition manager and his staff, as well as defense contractors and government end users with a detailed explanation of the CALS program, its objectives and strategy, and how to develop and apply CALS requirements that meet the needs of a particular weapon system development program. The current version is `B`.

MIL-SPEC (Military Specification): A Specification used to specify requirements when designing or producing a product for the Department of Defense.

MODEM (MOdulator-DEModulator): A device that converts digital signals from a computer to analog signals for transmission over phone lines.

Mosaic: Windows-like product for exploring the Internet that is available free in Cyberspace, CompuServe, America On-line, and many bulletin boards. Mosaic was developed by the National Center for Supercomputing Applications at University of Illinois and was funded with tax dollars.

Motif: Graphical user interface specified by the Open Software Foundation and built on the Massachusetts Institute of Technology's X Windows.

MPEG (Motion Pictures Experts Group): An emerging standard for compression of full motion images driven by the same committee as the Joint Photographic Experts Group (JPEG) standard.

jwagner74@juno.com

APPENDIX SIX

MRP (Material Requirements Planning): Original manufacturing business software that focused only on planning the manufacturing materials and inventories and did not integrate planning for other resources, such as people and machine capacity.

Multimedia: Used essentially to define applications and technologies that manipulate text, data, images and voice full motion video objects. Typically associated with PCs, but increasingly associated with networked-based applications.

National Information Infrastructure (NII): A concept conceived by the Clinton Administration and an alliance of computer, software, cable, and phone companies. The proposed concept would be the electronic network of tomorrow and would use phone line, cable systems, and high-speed data-networks to link everyone, including government agencies, universities, company presidents, and private citizens. The concept envisions vast amounts of services, entertainment, and information being made readily available through computers, televisions, telephones, and other means of electronic communication.

National Research and Education Network (NREN): The High-Performance Computing and Communications Act of 1991 (sponsored by Vice-President Gore) was a bill that created the NREN. NREN will use the Internet to provide information resource connection not only to universities, research centers and government agencies, but also to secondary and elementary schools. The bill provides $2.9 billion over a five year period towards the NREN. The High-Performance Computing and High Speed Networking Applications Act of 1993, sponsored by Rep. Richard Bouche, expands the Gore bill to also include access to health care facilities and schools at all levels.

Network Driver Interface Specification (NDIS): A Microsoft specification for a type of device driver that allows multiple transport protocols to run on one network card simultaneously.

Network News Transport Protocol (NNTP): An extension of the TCP/IP protocol that describes how newsgroup messages are transported between compatible servers.

Newsgroup: A BBS-like forum or conference area where you can post messages on a specified topic. Many newsgroups covering a wide range of topics exist on the Internet.

NIST (National Institute of Standards and Technology): Created in 1901 as the National Bureau of Standards and renamed in 1988, the National Institute of Standards and Technology (NIST) works to strengthen U.S. industry's international competitiveness, advance science, and improve public health, safety and the environment. NIST conducts science and engineering research in commercially important fields such as advanced materials, information systems, biotechnology, optoelectronics, computer-integrated manufacturing, and sensor technology.

Node: A Node is a termination point for two or more communication links. The Node serves as the control location for forwarding data among the elements of a network or multiple networks, as well as perform other networking, and in some cases, local processing functions. In systems network architecture, a node is an end point of a link or a junction common to two or more links in a network. Nodes can be host processors, communications controllers, cluster controllers, work group computers or terminals.

OCR (Optical Character Recognition): The ability of a computer to recognize written characters through some optical-sensing device and pattern recognition software.

ODA/ODIF (Office Document Architecture / Office Document Interchange Format): An explicit document architecture and interchange format standard which allows exchange of compound documents (i.e., documents composed of various content types, such as character, raster graphics, and geometric (Computer) graphics content.

Open Data-link Interface (ODI): A standard interface, developed by Novell and Apple, that performs the same functions as NDIS.

Open System: A system capable of communicating with other open systems by virtue of implementing common international standard protocols.

OSI (Open Systems Interconnection): A standard approach to network design developed by the International Standards Organization that introduces modularity by dividing the complex set of functions into more manageable, self- contained, functional slices.

Optical Disk: An unalterable optical storage medium that allows large amounts of data to be permanently written to it. An optical disk is read using laser and magnetic technology and has a useful life span of 100 plus years.

Packet Internet Gopher (PING): A TCP/IP utility that sends packets of information to a computer on a network. It can be used to determine if a computer is connected to the Internet.

jwagner74@juno.com

APPENDIX SIX

Parser: The word "parse" comes from "parts of speech" in Latin. It means to part or break down into component parts. A parser is a specialized software program that recognizes SGML and markup in a document. A parser that reads a DTD and checks and reports on markup errors is a validating SGML parser. A parser can be built into an SGML editor to prevent incorrect tagging and to check whether a document contains all the required elements.

PDES/STEP (Product Data Exchange Standard/Standard for the Exchange of Product Model Data): A set of standards under development for communicating a complete product model with sufficient information content that advanced CAD/CAM applications can interpret. PDES is under development as a national (U.S.) standard and STEP is under development as its international counterpart.

PDF (Portable Document Format): A file format created with Adobe Acrobat which ensures that the document looks the same on any computer equipped with a free Acrobat reader. PDF Writer lets you direct print output from a word processing or page layout pogrom to a PDF file instead of a printer. Using it is as easy as printing. Acrobat Exchange allows you to modify PDF documents by adding hypertext links, text, annotations, and security restrictions.

PDL (Page-Description Language): Software that instructs a printer in composing various elements (e.g., text, graphics, images) of a printed page. [Ed. or Standard Page Description Language: ISO 10180, Information Processing Text Composition], 1993.

One of the most popular PDLs is PostScript. PostSript documents can be printed at very high resolutions (600 dpi to 1200 dpi or more) depending on the capability of your printer.

PLDB (Parts List Data Base): This tool controls parts inventory during fabrication and operation. PLDB provides inventory status of parts, prepares part list reports, generates purchase orders, and tracks cost/budget of parts. PLDB is linked to LSAR, Imaging, and Bar Coding.

POSIX (Portable Operating System Interface): This standard defines a C programming language source interface to an operating system environment. This standard is used by computing professionals involved in system and application software development and implementation.

POTS: Plain old telephone service. An unenhanced voice quality connection.

PREMO: A proposed international standard that specifies techniques for creating audiovisual interactive applications that recognize and emphasize the interrelationships among user interfaces, multimedia applications, and multimedia information interchange. PREMO includes interfaces for external storage, retrieval, and interchange of multimedia objects. The objective of PREMO is to consider the needs of the computer graphics community in the mid-1990s, including new application areas.

Processable Data Document: Technical data in digital source form that is either organized and formatted so that an automated data processing system can further structure or restructure the data in a variety of ways, or is compatible for direct processing by an automated design, engineering, or logistic support system. Processable data can be updated or transformed for other applications such as production of document images.

Product Data: All engineering data, in processable form, necessary to define the geometry, the function, and the behavior of an item over its entire life span, including logistic elements for quality, reliability, maintainability, topology, relationship, tolerances, attributes, and features necessary to define the item completely for the purpose of design, analysis, manufacture, test, and inspection.

Product Model: A data model that contains the functions and physical characteristics of each unit of a product throughout its complete life cycle (from requirements specification to disposal).

Propriety Standard (Defacto Standard): A standard which has been endorsed by industry or government as the accepted international standard, but not officially approved by an accredited standards body such as ISO.

Protocol: A set of procedures for establishing and controlling data transmission. Examples include IBM's BSC (Binary Synchronous Communications) and SDLC (Synchronous Data Link Control) protocols.

Protocol: A set of rules (priorities) and exception handlers for managing the communications on a network. A set of rules or standards that describes ways to operate to achieve compatibility. Alternatively, A mutually determined set of formats and procedures governing the exchange of information between systems.

Query Language: A defined set of syntax and commands used to submit queries to a text retrieval system.

RAMP (Rapid Acquisition of Manufactured Parts): The Navy's RAMP program will enhance logistic support by applying data-driven automated manufacturing, acquisition, and inventory management technologies to produce small

lots of selected, hard-to-acquire parts and assemblies at reduced cost and significantly shortened lead times.

Random-Access Memory (RAM): Thought of as temporary memory because when the computer is turned off, all data stored in RAM is lost. To run a computer software application, it must be loaded into RAM. All computer programs (software) have a minimum RAM requirement.

Rapid Response Manufacturing (RRM): One of the major objectives of RRM is to create an engineering information environment that is accessible and useful for multiple engineering and manufacturing applications. Accepted robust standards for process and product data storage and exchange, which commercial vendors actively support, are a necessary ingredient of the infrastructure being developed within the RRM program. RRM views the continuing development and access of STEP as crucial.

Raster Graphics: A method of representing a two-dimensional image by dividing it into a rectangular two-dimensional array of picture elements (pels), achieved by scanning.

RDA (Remote Data Access): A standard being developed to interconnect applications and databases. The standard originally attempted to cover any kind of data access and concerned itself only with effective dialogue management, but the complexity of so broad a scope has focused it more on Structured Query Language (SQL). An SQL specialization draft based on SQL2 is being developed as the first potential implementation of RDA.

RDBMS (Relational Database Management System): A database management system in which the database is organized and accessed according to the relationships between data items. In a relational database, relationships between data items are expressed by means of tables. Interdependencies among these tables are expressed by data values rather than by pointers. This allows a high degree of data independence.

Real-Time: The description for an operating system that responds to an external event within a short and predictable time frame. Unlike a batch or time-sharing operating system, a real-time operating system provides services or control to independent ongoing physical processes.

Relational Database: A database system in which the database is organized and accessed according to the relationships between data items without the need for any consideration of physical orientation and relationship. Relationships between data items are expressed by means of tables.

Reliability: The duration or probability of failure-free performance under stated conditions; or the probability that an item can perform its intended function for a specified interval under stated conditions.

Repository: A facility for storing descriptions and behaviors of objects in an enterprise, including requirements, policies, processes, data, software libraries, projects, platforms and personnel, with the potential of supporting both software development and operations management. A single point of definition for all system resources.

Resolution: The clarity of a monitor screen. Resolution is expressed in pixels. The more pixels there are, the higher the resolution.

A document issued by the government to request bids for products or services.

RFQ (Request For Quote): Request For Quote is a request issued by a contracting agency to industry for quotes (proposal) in support of goods or services.

ROM (Read-Only Memory): A type of computer storage that is not available to the user for writing. That is, the user of ROM can access and use data which is stored in ROM, but can not change the data. Computer CDs use ROM. Once data is placed in ROM it remains and can not be altered in any way by the user.

Router: Hardware/software solution that directs messages between LANs.

Search Engine, Tool, Utility: A remotely accessible program that lets you do keyword searches for information on the Internet. The search engine is a server program and should not be confused with the browser or other programs that run on your desktop PC. There are a number of search utilities for the WWW (Yahoo, Lycos, etc.). The other Internet services typically have one search tool: (FTP--Archie, Gopher--Veronica,...)There are several types of search engine; the search may cover titles of documents, URLs, headers, or the full text.

Serial Line IP/Point-to-Point Protocol (SLIP/PPP): Two protocols that allow dial-up access to the Internet through a serial link. Most Internet access packages support both, through you can use only one at a time.

SGML (Standard Generalized Markup Language):

A *markup language* uses tags to indicate changes within a document, changes in presentation style, or changes in

content type. *Generalized* means that the markup used to describe a document is based on the content of that document, not on its appearance. *Standard* means that the language has gone through the international standards process. The SGML standard, approved in 1986, defines a language for document representation which formalizes markup and frees it of system and processing dependencies. It provides a coherent and unambiguous syntax for describing whatever a user chooses to identify within a document.

SGML is a metalanguage, a way of talking about (and testing or validating) lower level languages. In the case of SGML it might be a way of talking about elements and tags used in DTDs (document type definitions). To apply SGML, one first defines a document type. The definition would tag all the page elements that would deserve special considerations. Bracketed tags mark the beginning and end of each element. HTML 3.0 is an SGML DTD.

Simple Mail Transfer Protocol (SMTP): A protocol that describes how information is passed between reporting devices and data collection programs. It can be used to gather information about hosts on the Internet.

Source System: The computer hardware, software, and network that will structure technical information for interchange.

SQL (Structured Query Language): SQL is a relational data language that provides a consistent, English keyword-oriented set of facilities for query, data definition, data manipulation and data control. It is a programming interface to a relational database management system (RDBMS).

Standards Testing: Determines whether the national, international, or military standards (and specifications) are viable and implementable.

STEP (Standard for the Exchange of Product model data): A standard under development which will be used to describe a product in a neutral format over its complete life-cycle in a hardware-independent way. Source: Department of Trade and Industry, United Kingdom. "CALS: Computer Aided Acquisition and Logistic Support: The Executive Guide. "

System: Specific suite of computer hardware and software. As used in the terms "Source System" and "Destination System," the term does not necessarily correspond one to one with "site" or "base" in that most prime contractor sites and DoD installations have more than one system.

Tape Set: A group of one or more magnetic tapes which collectively represent the collection of related files comprising a specific delivery of a document or documents.

TBITS (Treasury Board Information Technology Standards): Treasury Board Information Technology Standards are the official Government of Canada publications on the standards, guidelines, technical reports and standard operating practices adopted and promulgated under the Treasury Board Information Management policies.

TDP (Technical Data Package): A technical description that is adequate to support acquisition of an item, including engineering and production, the description consisting of all applicable technical data such as engineering drawings, associated lists, product and process specifications and standards, performance requirements, quality assurance provisions, and packaging details.

Technical Data: Recorded information, regardless of form or method of the recording of a scientific or technical nature (including software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

Technical Information Systems: The generic term for the enterprise network of existing and augmented automated data processing systems used by government and contractors for management of technical information in support of the design, manufacture, and logistic processes for products such as weapon systems and related major equipment items.

Telnet: A terminal emulation protocol that allows remote log in from any computer on an internet. Once logged on you can retrieve files from or send files to that remote computer. (2) A portion of the TCP/IP suite of software protocols that handles terminals. Among other functions, it allows a user to log in to a remote computer from the user's local computer.

Text File: A file which uses the American Standard Code for Information Interchange (ASCII) or similar system to represent the text of a document. Data within a text file are delineated as human readable words, sentences, and paragraphs rather than data elements.

Text-Graphics Integration: The necessary indexing and linkages between a computer readable text file and a separate

computer readable graphics file, or graphics subsection of the same text file, such that both portions can be output or updated as a single, apparently continuous, unit.

TIFF (Tag Image File Format): a de facto standard format for image files. The standard used by all FAX machines.

Total Quality Management (TQM) : Interfunctional approach to quality management, developed by Joseph Juran, involving marketing, engineering, manufacturing, purchasing, etc. Defects should be defined through examining customer expectations. The focus is on prevention, detection, and elimination of sources of defects. The Juran total quality management trilogy is quality control, quality planning, and quality projects.

Transmission Control Protocol/Internet Protocol (TCP/IP): A compilation of network and transport level protocols that allow a PC to speak the same language as other PCs on the Internet or other networks.

Unix: A family of operating systems known for its relative hardware independence and portable applications interface.

Usenet (User Network): A public network made up of thousands of newsgroups and organized by topic.

VAN (Value-Added Network) : A system where a network leases communication lines from a communications common carrier, enhances them by adding improvements such as error detection and/or faster response time, and then allows others to use this service on those lines for a fee.

Vector Graphics: The presentation of images stored as line segments or other mathematical representations.

Very Easy Rodent-Oriented Netwide Index to Computerized Archives (Veronica): A search tool (like archie) that searches text that appears in Gopher menus.

WAN (Wide-Area Network): A data transmission facility that connects geographically dispersed sites using long-haul networking facilities.

Web Browser: *(see client software, browser)*A World Wide Web client. PC Software such as Netscape Navigators or NSCA Mosaic that serves as an information retrieval tool. The browser locates the web site specified in a URL, transfers the specified file, and interprets the HTML code.

WHOIS: A TCP/IP utility that lets you query compatible servers for detailed information about other Internet users.

Wide Area Information Server (WAIS): Software that is used to index large text files in servers. On the client side, it finds and retrieves documents in databases, based on user-defined keywords. WAIS indexes can be searched for everything from government documents and treaties to documents about obscure religious sects.

Workflow Management: A software application that controls the order and monitors the execution of a series of processes (worksteps) in which people act upon work items (documents, forms, folders and images).

Workflow: The automation of work among users where the system is intelligent enough to act based on definition of work types, users, tasks and the recognition of dynamic processing conditions.

World Wide Web (WWW): A network of servers that uses hypertext links to find and access files. Many Web sites also support video and sound.

X 12: ANSI X12 Ver. 3050 transaction sets can be described in six pages of 3 digit codes. The X12 format standard is commonly used in EDI (automated computer to computer data exchange). Purchasing transaction sets include **840**s RFQs, **850**s Purchase Orders, **855**s PO Acknowledgements. Financial transaction sets include **810**s Invoices.

X.25: A data communication protocol that ensures data integrity while data is being transmitted to, from and within the network. This standard defines the interconnection of packet-switching networks and their associated computers or terminals. These types of networks make efficient use of the telecommunications networks by taking the data generated by a computer or a remote terminal and chopping it up into small identified packets and then looking for the most efficient way of sending this information to its destination.

X.400: Defines the special rules for transmission of a message which may include text, pictures, and graphics, and allows information to be transmitted between computers, without specific manufacturer restrictions.

X.500: The establishment of any global interconnected network, requires a directory. The standard for establishing such a directory is X.500, which enables users to browse through user listings as though they were looking through a telephone book.

BIBLIOGRAPHY

Paliotta, Allan R. "Cybersecurity and the Future of e-Commerce" *IS Audit and Control Journal, Volume II (2001):* http://www.isaca.org

Ghosh, Anup K *Security and Privacy for e-Business* (New York: John Wiley & Sons, 2001)

Checklist for Auditors: e-Commerce Project Risk, (United Kingdom: Ink-e Media, September 2001)

Deloitte & Touche, *e-Commerce Security-Public Key Infrastructure: Good Practices for Secure Communications* (Rolling Meadows, Illinois: Information Systems Audit and Control Foundation, 2001)

Lundquist, Eric "Security: That Most Thankless of Tasks" *PC Week* (2001): http://www.zdnet.com/eweek

IT/Middle Management Conference (Nashville, Tennessee: National State Auditors Association, 2001)

Scambray, Joel; McClure, Stuart; and Kurtz, George *Hacking Exposed: Network Security Secrets and Solutions, Second Edition* (Berkeley, California: McGraw-Hill, 2001)

Gonzalez, Marcelo Hector "Banks and the Possibilities of e-Commerce" *IS Audit and Control Journal, Volume IV* (2001): 55-56

Cangemi, Michael P. "Internet Security Policy Forum" *IS Audit and Control Journal, Volume IV* (2001): http://www.isaca.org

Stein, Douglas; Arunachalam, Vairam; and Rittenberg, Larry "Electronic Commerce System Sophistication and the Audit Process: Insights from Information Systems Auditors" *IS Audit and Control Journal, Volume I* (2001): http://www.isaca.org

Harrison, Brendan "Breaking the Code: September's Terrorists Attacks on the US have Raised Concerns About Encryption Technology" *Offshore Finance USA* (November/December 2001): 18, 65

North American Conference on Audit, Control, and Security (Orlando, Florida: Information Systems Audit and Control Association, 2001)

Third Annual Network Security Conference (Las Vegas, Nevada: Information Systems Audit and Control Association, 2001)

University of New Haven Center for Cybercrime and Forensic Computer Investigation and the University of South California Department of Mathematics "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security" *IS Audit and Control Journal, Volume II (2001):* http://www.isaca.org

Harreld, Heather and Fonseca, Brian "Guarding Against Cyberterrorism" *Infoworld* (October 22, 2001): 32-37

Chidi, George A. Jr., "FCC Creates Homeland Security Policy Counsil" *Computerworld* (November 15, 2001): (http://www.computerworld.com)

Verton, Dan "Users are the Weakest Link, Security Experts Warn" *Computerworld* (November 15, 2001): (http://www.computerworld.com)

Verton, Dan "Analysts: Insiders May Pose Security Threat" *Computerworld* (October 14, 2001): 6

Certified Information Systems Auditor (CISA) Technical Information Manual (Rolling Meadows, Illinois: Information Systems Audit and Control Association, 2000)

COSO Internal Control Training (Springfield, Illinois: KPMG, LLP, 2000)

Meritt, James W. *A Method for Quantitative Risk Analysis* (http://www.auditnet.org, 1999)

Internal Control Issues in Derivative Usage http://www.coso.org

Internal Control - Integrated Framework http://www.coso.org

Deloitte & Touche, *e-Commerce Security-A Global Status Report* (Rolling Meadows, Illinois: Information Systems Audit and Control Foundation, 2000)

Deloitte & Touche, *e-Commerce Security-Enterprise Best Practices* (Rolling Meadows, Illinois: Information Systems Audit and Control Foundation, 2001)

Martin, Denys "Risk Assessment When Auditing e-Commerce Activities" *Institute of Internal Auditors IT Audit Forum* (2000): http://www.itaudit.org

jwagner74@juno.com

Crume, Jeff *Inside Internet Security: What Hackers Don't Want You to Know* (Harlow, England: Addison-Wesley, 2000)

Mehta, Raj "Secure e-Business" *IS Audit and Control Journal, Volume I* (2000): 32-37

Powers, William J. *Security Program for Electronic Data Interchange (EDI)* (MIS Training Institute, 2001)

Mahadevan, Chidambaram "Intrusion, Attack, Penetration-Some Issues" *IS Audit and Control Journal, Volume VI* (2001): 52-57

IS Audit and Security Acronym Dictionary (MIS Training Institute, 2000)

Applegate, Dennis and Willis, Ted *Struggling to Incorporate the COSO Recommendations Into Your Audit Process?* (The Institute of Internal Auditors, 1999)

Oliphant, Alan "An Introduction to Computer Auditing - part 4" *Institute of Internal Auditors* (January 1, 1999): http://www.itaudit.org/public_forum/f103na.htm

Cullinane, David "Electronic Commerce Security" *Handbook of Information Security Management* (New York: Auerbach, 1999): 219-236

Applegate, Dennis and Willis, Ted "Struggling to Incorporate COSO Recommendations Into Your Audit Process? Here's One Audit Shop's Winning Strategy" *Internal Auditor* (1999): http://www.theiia.org

Federal Information System Controls Audit Manual (FISCAM) (United States General Accounting Office (GAO), 1999)

Federal Information Processing Standards (FIPS) (United Stated Department of Commerce/National Institute of Standards and Technology, 1998)

Nagel, Karl D. and Gray, Glen L. *Miller Electronic Commerce Assurance Services* (San Diego: Harcourt Brace Professional Publishing, 1999)

Rion, Michael and Gebing, Robert "Doing the Right Things" *Internal Auditor* (December 1999): 33-35

jwagner74@juno.com

Collins, Rod “Auditing in the Knowledge Era” *Internal Auditor (June 1999):* 26-31

"Risk and Controls in an EDI Environment" *IS Audit and Control Journal, Volume V* (1998): 40-43

Oliphant, Alan "An Introduction to Computer Auditing - part 2" *Institute of Internal Auditors* (October 1, 1998): http://www.itaudit.org/public_forum/f103na.htm

Marcella, Albert J. Jr; Stone, Larry; and Sampias, William J.; *Electronic Commerce: Control Issues for Securing Virtual Enterprises* (Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation, 1998)

Ghosh, Anup K *e-Commerce Security: Weak Links, Best Defenses* (New York: John Wiley & Sons, 1998)

Control Objectives for Information and Related Technology (CobiT), (Rolling Meadows Illinois: ISACF, 2000)

Digital Signature Standard (United States Department of Commerce/National Institute of Standards and Technology, 1998)

Gallegos, Frederick and others, eds., *Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Levels* (Rolling Meadows, Illinois: ISACF, March 1998)

Colbert, Janet L. and Bowen, Paul "A Comparison of Internal Controls: CobiT, SAC, COSO, and SAS 55/78” IS *Audit and Control Association* (1998): http://www.isiaca.org/bkr_cbt3.htm

Performance Audit Manual, September 1998

Electronic Money: Consumer protection, law enforcement, supervisory and cross border issues. Report of the working party on electronic money (Switzerland: Bank for International Settlements, April 1997)

Russel, Larry "How electronic commerce is changing the way we do business" *Outlook,* (Spring 1997): page S8

Garfinkel, Simson and Spafford, Gene *Web Security and Commerce* (Beijing: O’Reilly & Associates, 1997)

jwagner74@juno.com

CPA Journal (December 1996) pages 13-16

Simmons, Fred *Network Security: Data and Voice Communications* (New York: McGraw- Hill, 1996)

Pushkin, Morris and A. B. "Contributions of IS Auditors to the Development of EDI Systems" *IS Audit and Control Journal, Volume VI* (1996): 34-39

Garceau, C. Foltin "Neural Networks: A New Technology and the Impact on IS Auditors" *IS Audit and Control Journal, Volume II* (1995): 52

"General Standards for Information Systems Auditing and Statements 1-9 on Information Systems Auditing Standards" EDP Auditors Foundation, Inc. *IS Audit and Control Journal, Volume I* (1994): 60

COSO Internal Control-Integrated Framework Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission (1992)

"Computer Issues in the use of Electronic Data Interchange" *Computer Systems Laboratory (CSL) Bulletin*, (June 1991): 1-6

Systems Auditability and Control, (Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation, 1994)

Control Objectives, (Rolling Meadows Illinois: Information Systems Audit and Control Foundation (ISACF), 1990)

Murphy, Michael A. and Parker, Xenia Ley *Handbook of EDP Auditing, Second Edition* (Boston: Warren Gorham & Lamont, Inc., 1989)

National Commission on Fraudulent Financial Reporting, *Report of the National Commission on Fraudulent Financial Reporting* (http://www.coso.org, 1987)

Hayes, Frank "Sanity Check Please" *Computerworld* (September 13, 1999): http://www.computerworld.com