INFORMATION SYSTEMS AUDITING AND ELECTRONIC COMMERCE

Dr. M. Prakash*

D. Sivakumar**

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 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 article was threefold. First, the articles 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 article 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."*

Keywords: *Information System Auditing, Electronic Commerce, and e-commerce.*

*Head & Supervisor, Department of Commerce, PEE GEE College of Arts & Science, Periyanahalli, Dharmapuri, TamilNadu.

**M.Phil Research Scholar

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.

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.

- 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 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 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 “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:

- 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
- 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 specific areas of computer auditing which are independent of technology. These basic areas can be summarized as

- 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

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

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

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 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.

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.

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. 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. 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. We have all done it: given a waiter a credit card, and let it out of our sight long 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), alsoknown as the Information Systems Audit and Control Foundation. 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.

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 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.

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

- 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 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 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." 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" 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.

- 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
- 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 specific areas of computer auditing which are independent of technology. These basic areas can be summarized as

- 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

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

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

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 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.

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.

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.

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.

REFERENCES

1. Internal and External Audits Comptroller's Handbook July 2000.
2. Information Systems Auditing and Assurance – James A Hall, South Western College
3. Financial Accounting – Meigs & Meigs and Bettner and Whittington, Irvin McGraw Hill.2000
4. Information Technology Act, 2000 dated the 17th October, 2000 –Government of India
5. Information Technology (Certifying Authorities) Rules, 2000 dated the 17th October, 2000 – Government of India