

The Role of Information Technology On Information System Auditing Process of Business Networking

Henricus Bambang Triantono
Fakultas Bisnis dan Manajemen
Universitas Widyatama

Abstract

This article provides an overview of the role of IT on the audit process of business networking. Even when a client's use of IT leads to top enhanced internal control, the use of IT- based accounting systems introduces new risks typically not associated with traditional manual systems. Well-managed companies recognize these new risks and respond by implementing effective general and application controls in the system to reduce the impact of those risks on financing reporting. The auditor must be knowledgeable about these risks and obtain an understanding of the client's general and application controls to effectively plan an audit. Obtaining knowledge about general controls provides a basis for the auditor to rely on applications controls. Some of the auditor's test of controls can be performed by the computer, often as a way to achieve more effective and efficient audits. Reliance on general and application controls to reduce control risk is likely to change when clients use microcomputers, networks, database management systems, e-commerce systems, and outsourced computer service centers instead of centralized IT systems.

Key words: Information Technology, Information System, the audit process,

1. Introduction

This paper explores the use of information technology for audit automation purposes in the process of business networking. The use of information technology in the audit process of business networking has greatly increased in the last few years. This is especially the audit process for the audit firms who have been motivated by the desire to improve efficiency in order to compete with each other for clients. The principal method by which efficiency gains may be made is through the substitution of capital for labor. Although it is invariably the policy of the audit process business networking audit firms in the Institutions.

An organization in the process business networking must control and audit computer-based information systems because the cost of errors and irregularities that arise in these systems can be high. An organization's ability to survive can be severely undermined through corruption or destruction of its database; decision making errors caused by poor-quality information systems; losses incurred through computer abuse; loss of valuable computer hardware and software and personnel; the high costs of some types of computer errors; failure to maintain the privacy of individual persons; and failure to control how computers are used within the organization.

But the increased use of information technology is not the only strategy being adopted by the audit firms to cope with a more competitive environment. There has been a move away from systems and transactions audits to risk-based auditing which concentrates the effort of the audit team on those parts of the client's' business with the highest audit risk. As a consequence, risk-based auditing tends to rely more on the experience and judgment of managers and partners than on traditional programmed audit procedures normally conducted by assistants and seniors. Many of the tasks undertaken by audit staff might be characterized as being low-skilled, tasks which could be undertaken by staff without any training in accounting or audit. This has implications not only for the work roles of graduate audit staff but also secretarial and clerical staff, many of whose tasks are now undertaken by the audit staff.

Audit firms have been at the forefront of the use of microcomputers for many years, especially for accounts preparation, and more recently there have been a number of applications used in the audit process. These applications are normally grouped together under the heading of audit automation, which one semi-official publication has defined as:

"The use of computers in the management, planning, performance and completion of audits to eliminate or reduce time spent on computational or clerical tasks, to improve the quality of audit judgments, and to ensure consistent audit quality" (Audit Automation, 1992)

In addition to these benefits the same publication suggests that audit automation can improve motivation, job satisfaction and performance of staff by eliminating tedious or unproductive audit steps. Audit automation can also free audit staff for analytical rather than clerical tasks and hence facilitate the provision of a quality service to clients. Nor is this all. Audit automation can enhance client perceptions of the quality of the audit service and it can develop improved computer literacy in staff. From the above brief discussion it is clear that audit automation has a lot to live up to.

Theoretical Framework

Theory framework to explain divided to the two part of that is Organization Business Networking Based IT-THE Basic Data on of Processing Configurations. At picture part of this explained by how activity aspects in a business network organization being based on TI. Here in after at part of next picture wish to be shown how Impact IT of process of IS auditing in a network organization work business happened.

Before proceeding to explain the other aspects of Information System Auditing, it may be helpful to consider the basic diagram shown in Figure below, which establishes the usual functions within a data processing department using a disk/ tape-based third generation mainframe computer, with no terminal access. Although most modern systems incorporate the use of terminals, the illustration is useful as an introductory position, enabling us to understand the principles involved and dealing later with problems relating to terminals and microcomputers.

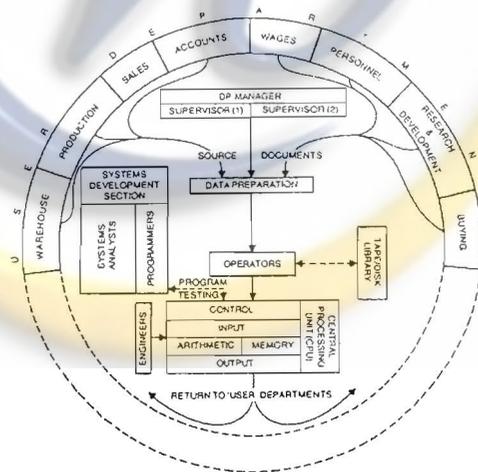


Figure 1. Organization Business Networking Based on IT
The Basic Data Processing Configurations

Apart from identifying the job titles and functions of personnel in the DP section, which occupies the central area, the diagram also symbolizes the relationship between external ('user') departments and the DP section. This has significant internal control, and hence audit, implications which we shall consider later in the figure. Many modern systems, unlike that portrayed in figure, would now employ terminals in each department so that centralized data preparation is avoided, each department having access to the central processing unit at specific times.

2. Overview of IS Auditing

IT usages have expanded very quickly and have a big impact to modern life. With existence of growth of this technology, its impact of accountant profession includes:

- a. Auditor shall have knowledge and understand the information technology. A Chairman of national accountant office [in] America tell "... *The Accountant expert computer a be to have will tomorrow of. And tomorrow is already here.*
- b. If network work business use system of EDP complicated, auditor have to have technical knowledge of goodness about its audit system. Without existence of knowledge concerning computer, auditor will not can make correct consideration as well as will not earn to conduct duty accumulate data/ needed evidence better.

Computers are used extensively to process data and provide information for decision making. They were available only to large business networking that could afford their high price and operation costs.

2.1 IS Auditing Defined

According to Weber, *Information systems auditing is the process of collecting and evaluating evidence to determine whether a computer systems safeguard assets, maintains data integrity, allows organizational goals to be achieved effectively, and uses resources efficiently* (Weber, 1999). Thus, information systems auditing (IS Auditing) supports traditional audit objectives: attest objectives (those of the external auditor) that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditors) that encompass not only attest objectives but also effectiveness and efficiency objectives.

According to this definition, IS Auditing is the evaluation of computer information systems, practices, and operations to assure the integrity of an entity's information. This evaluation can include the assessment of how efficient, effective, and economical computer based practice are. This includes the use of the computer as and audit tool. Also the evaluation should determine the adequacy of internal control within the CIS environment to assure valid, reliable, and secure information services.

Sometimes IS auditing has another objectives namely, ensuring that an organization complies with some regulation, rule, or condition. For example, a bank might have to comply with a government regulation about how much it can lend.

In this light, Figure below that throughout this case we conceive IS auditing as being a force that enables organization to better achieve four major objectives. We consider each of these objectives in detail.

Figure Role Function of IS Auditing at Organization.

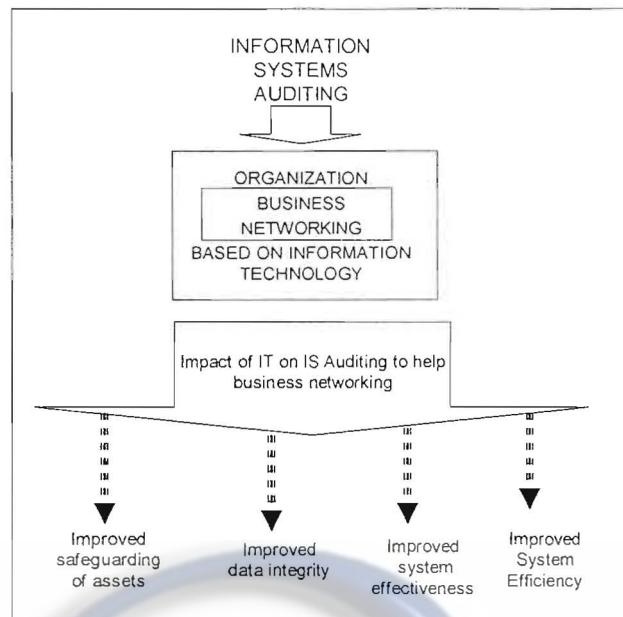


Figure 2. Borrowed Ideas From: Ron Weber, IS Control and Make an audit of Prentice Hall, 1999 which modified.

System Internal Control in EDP/ IS Auditing, According to Norm book Inspection of Accountant or Professional Standard of Public Accountant (taken away from SAS No. 1 AUSEC 320.09), internal control system cover organizational plan and also all coordinated rule and method which embraced in a company:

1. To protect its property
2. Checked careful and data reliability of accounting,
3. The increasing of efficiency of effort ,
4. Pushing adhering of policy of management which have been marked with lines.

Data-processing systems which have the character of manual differ from data-processing system which has the character of electronic/ computer. For the reason hence assessment procedure to its internal control system also will influence by this occurrence.

2.2. Needed for control and audit of computer

Computer in this time used widely either by big scale company and also small and medium scale company. Growth of and hardware of software fast computer make competition also mount, spreading of knowledge of computer which will quickly still will continue to continue and that influence worldwide economy.

Since computer used widely to process data and yield information to be used for decision making, hence require to be conducted by operation to computer usage.

There is seven causes needing of audit and operation to computer, that is:

- 1) Organizational costs of data loss
- 2) Incorrect decision making
- 3) Cost of computer abuse

- 4) Value of computer hardware, software and personnel
- 5) High costs of computer error
- 6) Maintenance of Privacy
- 7) Controlled Evolution of Computer use

Organizational costs of data loss. Data make up a critical resource necessary for an organization's continuing operations. In this regard, Everst (1985) proposes that data provides the organization with an image of itself, its environment, its history, and its future. If this image is accurate, the organization increases its abilities to adapt and survive in a changing environment. If this image is accurate or lost, the organization can incur substantial losses.

Such losses data can occur when existing controls over computers are lax, management might not provide adequate back for computer files. The loss of a file through computer program error, sabotage, or natural disaster means the file cannot be recovered, and the organization's continuing operations are thereby impaired.

Incorrect decision making. The importance of accurate data in a computer system depends on the types of decisions made by persons having some interest in organization. For example, if managers are making strategic planning decisions, they will probably tolerate some errors in the data, given the long-run nature of strategic planning decisions. If managers are making management control and operational control decisions, however, they will probably require highly accurate data. These types of decisions involve detection, investigation, and correction of out-of-control processes. Thus, inaccurate data can cause costly, unnecessary investigations to be undertaken or out-of-control processes to remain undetected.

Cost of computer abuse. Besides that, the major stimulus for development of the information systems audit function within organizations often seems to have been computer abuse. Parker (1970, p. 12) defines computer abuse to be "any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain.

Some major types of computer abuse that an organization are hacking, viruses, illegal physical access, and abuse of privileges. Computer abuse usually is a less serious problem for organizations than errors and omissions in computer systems or the effects of natural and human made disasters. Computer abuse can lead to the following types of consequences of abuse likes destruction of assets, theft of assets, modification of assets, privacy violations, disruptions of operations, unauthorized use of assets and physical harm to personnel.

Value of Computer Hardware, Software, and Personnel. In addition to data, computer hardware, software, and personnel are critical organizational resources. Some organizations have multimillion dollar investments in hardware. Even with adequate insurance, the intentional or unintentional loss of hardware can cause considerable disruption. Similarly, software often constitutes a considerable investment of an organization's resources. If the software is corrupted or destroyed, the organization might be unable to continue operations if it cannot recover the software promptly. If the software is stolen, confidential information could be disclosed to competitors; or, if the software is a proprietary package, lost revenues or lawsuits could arise. Finally, personnel are always a valuable resource, particularly in light of an ongoing scarcity of well-trained computer professionals.

High costs of Computer Error. Computers now automatically perform many critical functions within our society. For example, they monitor the condition of patients during surgery, direct the flight of missile, control a nuclear reactor, and steer a ship on its course. Consequently, the cost of computer error in terms of loss of life, deprivation of liberty, or damage to the environment can be high. For example, data errors in computer system used to control flight paths resulted in the death of 257 people when airplane crashed into a mountain in Antarctica; a person was jailed incorrectly for five months because of erroneous data contained in computer system.

Maintenance of Privacy. Much data is now collected about us as individual's likes taxation, credit, medical, educational, employment, and residence. This data was collected before computers. Nonetheless, the powerful data processing capabilities of computers, particularly their rapid

throughput, integration, and retrieval capabilities, cause many people to wonder whether the privacy of individuals (and organizations) has now been eroded beyond acceptable levels.

Controlled Evolution of Computer Use. Many people are concerned about the effects that use of computers can have on a person's working life. Should computer technology be allowed to displace people from the workforce or stultify jobs? What effects do computers have on the physical and mental well-being of their users? It might be argued that technology is neutral it is neither good nor bad. The use of technology, however, can produce major social problems. In the light, important, ongoing decisions must be made about how computers should be used in our societies. Governments, professional bodies, pressure groups, organizations, and individual persons all must be concerned with evaluating and monitoring how we deploy computer technology.

3. Discussion

3.1. Role of General Controls on Control Risk

Before discussed about IS Audit based on IT, we described general control and applications control, which part of an IS audit.

Most auditors evaluate the effectiveness general controls before evaluating application controls. If general controls are ineffective, there is potential for material misstatement in each computer-based accounting application, regardless of the quality of application controls. General control an organization includes the following organization planning EDP and operational activities, document procedure, software controls, access controls, and data controls procedure. Applications controls include the following inputs controls, processing controls and output controls. For example, if duties are inadequately segregated such that computer operators are also programmers and have access to computer programs and files, the auditor should be concerned about the potential for fictitious transactions or unauthorized data and omissions in accounts such as sales, purchases, and salaries. Similarly, if the auditor observes that data files are inadequately safeguard, the auditor may conclude that there is significant risk of loss of data because the general controls affect each application. In this situation, audit testing to satisfy the completeness objectives may need to be expanded in several areas such as cash receipts, cash disbursement and sales.

On the other hand, if good general are in place, there is an increased likelihood of placing greater reliance on application controls. Auditors can therefore test specific application controls for operating effectiveness and rely on the result to reduce substantive testing. This use of effective general and application controls can result in significant audit efficiencies.

One challenge, however, in IT environments is the impact of changes in software on the auditor's reliance on controls. When the client changes the software, the auditor must evaluate whether additional testing is needed. If general controls are effective, the auditor will be able to easily when software changes are made. In environments where general controls are weak, there is greater likelihood of unidentified changes in application software. As a result, auditor must concerned basic throughout the year when general controls are weak.

Auditors typically obtain information about general and application controls through interviews with IT personnel and key users; examination of system documentation such as flowcharts, user manuals, program change requests, and testing result; and review of detailed questionnaires completed by IT staff. In most cases, it is desirable to use several approaches in understanding internal control because each offers different information. Interviews with the chief information officer and systems analysts provide useful information about the operation of the entire IT function, the extent of software development and hardware changes made to key accounting application software, and an overview of planned changes. Reviews of program change requests and system test result are useful to identifying program changes in application software. Questionnaires are useful to identify specific internal controls. Based on those strengths and weaknesses, the auditor assesses control risk for each transaction related computer based auditing objective.

An organization must control and audit computer based IS because the cost of errors and irregularities that arise in these systems can be high. An organization's ability to survive can be

severely undermined through corruption or destruction of its database; decision making errors caused by poor-quality IS; losses incurred through computer abuse; loss of valuable computer hardware and software and personnel; the high costs of some types of computer errors; failure to maintain the privacy of individual persons; failure to control how computers are used within the organization.

The IS Audit function has been established to safeguard assets, to maintain data integrity, to achieve system effectiveness, and to achieve system efficiency. Following will be conducted by solution from each function in IS audit.

3.2. Improved safeguarding of assets

IS auditing can help improved safeguarding of assets. The information system assets of an organization include hardware, software, facilities, people (knowledge), data files, system documentation, and supplies. Like all assets, they must be protected by a system of internal control. Hardware can be damaged maliciously. Proprietary software and the contents of data files can be stolen or destroyed. Supplies of negotiable forms can be used for authorized purposes. These assets are often concentrated in one or a small number of locations, such as a single disk. As a result, asset safeguarding becomes an especially important objectives for many organizations to achieve.

3.3. Improved Data Integrity

Data integrity is a fundamental concept in information system auditing. It is a state implying data has certain attributes: completeness, soundness, purity, and veracity. If data integrity is not maintained, an organization no longer has a true representation of itself or of events. Nonetheless, maintaining data integrity can be achieved only at a cost. The benefits obtained should exceed the costs of the control procedure needed.

Three major factors affect the value of a data item to an organization and the importance of maintaining the integrity of that data item:

1. The value of the informational of the data item for individual decision makers
2. The extent to which the data items is shared among decision makers
3. The value of the data item to competitors

3.4. Improved System Effectiveness

An effective IS accomplishes its objectives. Evaluating effectiveness implies knowledge of user needs. To evaluate whether a system reports information in a way that facilitates decision making by its users, auditors must know the characteristics of user and the decision-making environment.

Effectiveness auditing often occur after a system has been running for some time. Management requests a post audit to determine whether the system is achieving its stated objectives. This evaluation provides input to decision on whether to scrap the system, continue running it, or modify it in some way.

Effectiveness auditing also can be carried out during the design stages of a system. Users often have difficulty identifying or agreeing on their needs. Moreover, substantial communication problems often occur between system designers and users. If a system is complex and costly to implement, management might want auditors to perform an independent evaluation of whether the design is likely to fulfill user needs.

3.5. Improved System Efficiency

An efficiency IS uses minimum resources to achieve its required objectives. IS consume various resources: machine time, peripherals, system software, and labor. These resources are scarce, and different application systems usually compete for their use.

The question of whether an IS efficient often has no clear-cut answer. The efficiency of any particular system cannot be considered in isolation from other systems. Problems of sub optimization

occur if one system is “optimized” at the expense of other system. For example, minimizing an application system’s execution time might require dedication of some hardware resource (e.g., a printer) so that system. The system might not use the hardware fully, however, while it undertakes its work. The slack resources will not be available to other application systems if it is dedicated to one system.

System efficiency becomes especially important when a computer no longer has excess capacity. The performance of individual application systems degrades, and users can become increasingly frustrated. Management must then decide whether efficiency can be improved or extra resources must be purchased. Because extra hardware and software is a cost issue, management needs to know whether available capacity has been exhausted because individual application systems are inefficient or because existing allocations of computer resources are causing bottlenecks. Because auditors are perceived to be independent, management might ask them to assist with or even perform this evaluation.

3.6. Roles of IT on IS Auditing

When first time EDP system, many auditor which feel that must be done elementary change to ordinary audit to be able to accommodate this new technology. In this time clear that auditor admit to use ordinary audit method to make an audit of although there computer.

Computer system give influence to two elementary function of audit, that is:

- a. collection evidence, and
- b. evaluation evidence.

3.7. Change to evidence collection.

Collect evidence able to be trusted when organization use more complex system computer when compared to use manual system. Auditor have to earn to collect evidence able to be trusted because many matter which not there are in manual system like the importance of test to program, control to used hardware.

Understanding of to operation of technology to computer is not easy to that thing happened because and hardware of software continually change and sometime the change happened quickly and radical. For example : by development usage of communications data to the transfer of data, substantial research into continuously development to control of cryptographic to protect data privacy, auditor have to keep abreast of this when them wish to have ability to evaluate communications network reliability.

Change of continuous technology make auditor progressively difficult to get evidence at some case, auditor cannot collect evidence make an audit of by using manual method so that needed computer system to auditor to be able to collect evidence make an audit of company using information system. Software development of needed general audit, for example: because auditor need data access through disk media hence audit of tools which is just needed auditor to can evaluate data communications network control reliability precisely, but development of audit of tools even also less at all.

3.8. Change to Evidence Evaluation

Growth of system of EDP also make auditor find difficulties to evaluate consequence of weakness and strength is overall of system able to be trusted. Mistake that happened at computer program make evaluation to evidence become something that very difficult and make auditor frustrated.

3.9. Foundations of IS Auditing

Requirement of function of IS make an audit of happened because two matters, that is

- a. Auditor realize that computer have had an effect on to ability of them to prove their function
- b. Network business organization and management confess that information technology represent valuable matter which must be controlled by like other resources.

Audit IS represent meeting four science discipline, that is a. traditional of auditing b. Management IS c. science behavioral. d. science computer.

Traditional audit pass to IS make an audit of congeniality to experience and ability about internal control technique. Knowledge and this experience give impact to process of design good of activity of machine component and also manual information system. For example, computer system, activity of clerical as activity prepare data oftentimes represent critical component system, like manual system. This activity have to represent internal operation subject like duty dissociation of function which compatible, owning capable employees and can be trusted and also the existence of dissociation of duty which top-drawer matter clearly. Perhaps which brought by traditional audit information system audit operation philosophy.

In the early usage of information system base on computer show many loss that happened, expenditure of very big expense and many unsuccessful system to reach target which have been specified. As its result is so much time year used by all researcher to concentrate on the way of to conduct good information system implementation and development.

Computer system sometime fail because people who design the system do not have appreciate to difficulty of arising out to human being which often happened implementation and development a system, for example, resistance of behavioral to information system can destroy seriously effort to take care of properties of organization, perfection of data, usage of system effectively and is efficient. Auditor have to earn to understand about the condition to be can overcome the problem of behavioral resulting system do not work, scientist behavioral especially deepening organizational theory which have important contribution to give congeniality to human being problem able to arise organization.

Computer of Scientist also have to concentrate on how to be target to take care of properties, data of integrity, system which efficient system and effective can reach better.

4. Summary and Recommendation

This paper studied the role of IT on the audit process business networking. Even when a client's use of IT leads to enhanced internal control, the use of IT-based accounting systems introduces new risks typically not associated with traditional manual system. Well-managed companies recognize these new risks and respond by implementing effective general and application controls in the IT system to reduce the role of those risks on financing reporting. The auditor must be knowledgeable about these risks and obtain an understanding of the client's general and application controls to effectively plan an audit. Obtaining knowledge about general controls provides a basis for the auditor to rely on application controls. Some of auditor's tests of control can be performed by the computer, often as away to achieve more effective and efficient audits. Reliance on general an application controls to reduce control risk is likely to change when clients use microcomputers, networks, database managements systems, e-commerce systems, and outsourced computer service centers instead of centralized IT systems.

IS auditing is an organizational function that evaluates asset safeguarding, data integrity, system effectiveness, and system efficiency in computer system. Asset safeguarding, data integrity, system effectiveness, and system efficiency can be achieved only if a sound system of internal control exists. Use of a computer for data processing does not affect the basic objectives of internal control; however, it affects how these objectives must be achieved.

The use of computers for data processing impacts both the evidence collection and evidence evaluation functions of auditors. Computer control technology is more complex than manual system

control technology; consequently, it is more difficult to understand controls and to collect evidence on the reliability of controls.

IS auditing borrows much of its theory and methodologies from other areas. Traditional auditing contributes knowledge of internal control practices and overall control philosophy. IS management provides methodologies necessary to achieve successful design and implementation of systems. Behavioral science indicates when and why IS are likely to fail because of people problems. Computer science contributes knowledge about control theory and the formal models that underlie hardware and software design as basis for maintaining data integrity.

5. Recommendation

Some quality which must have by someone to become IS Auditor, for example:

- Ability to evaluate objectively
- Ability to recognize key issues quickly
- Ability to communicate effectively
- Knowledge of the Computer Information System function

References

- Benbow, Gary(1990),”Computer Abuse in Australia,” *The EDP Auditor Journal*, II, 50-57.
- BloomBecker, J. J. Buck (1990), “Computer Crime and Abuse,” *The EDP Auditor Journal*, II, 34-41.
- Chambers, Andrew D (1981),” *Computer Auditing*”, The Pitman Press, London.
- Evens, Mark (1990),”Computer Security: What are the Risks?”*The EDP Auditor Journal*,II, 44-47.
- Everest, Gordon C. (1985), *Database Management: Objectives, System Functions and Administration*. New York: McGraw-Hill.
- Hirschheim Rudy, Heinz K.Klein, and Kalle Lyytinen (1995), *Information Systems Development and Data Modeling: Conceptual and Philosophical Foundations*. Cambridge: Cambridge University Press.
- Manson, Stuart., McCartney, Sean., Sherer , Michel., (1977), *The Use of Information Technology in The Audit Process*, Paper presented at offered for presentation at the Fith Interdisciplinary Perspectives on Accounting Conference University of Manchester.
- Parker, Donn B (1976), *Crime by Computer*, New York: Charles Scribner’s Sons.
- Redman, Thomas C.(1995),”Improve Data Quality for Competitive Advantage,” *Sloan Management Review* (Winter), 99-107.
- Strong, Diane M., Yang W.Lee, and Richard Y Wang (1997),”*Data Quality in Context*,” Communications of the ACM (May), 103-110.
- Weber, Ron (1999),” *Information Systems Control and Audit*”, Prentice Hall, Upper Saddle River, NJ 07458.