Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

A CONCEPTUAL FRAMEWORK FOR ONLINE INTERNAL CONTROLS

ASHUTOSH DESHMUKH
PENNSYLVANIA STATE UNIVERSITY – ERIE
avd1@psu.edu

ABSTRACT

The Internet and web based tools permeate almost every functional area of the business including supplier and customer relationships. The rise in business transactions over the networks is accompanied by explosion in various online controls. A profusion of online controls has created problems in understanding purposes and objectives of online internal controls. This paper presents conceptual approaches to the online controls to aid our understanding of controls on the Internet. First, COSO/AICPA framework is presented. The online internal controls are then classified according to this framework. This classification is useful to accountants and auditors in understanding the purposes of online controls. Next, a conceptual framework was developed based on the objectives of online internal controls, which is useful for managers. The objectives of internal controls were stated as validity of transactions, mutual authentication of identity, authorization, data integrity and confidentiality, non-repudiation, and auditability of transactions. This framework enables us to ask intelligent questions regarding internal controls even in the absence of full technical understanding of those controls.

Keywords: internal controls, security policies, online systems controls, security.

INTRODUCTION

The Internet and web have been firmly entrenched in today's business practices. The Internet and web based tools permeate almost every functional area of the business including supplier and customer relationships. Add to that a unique mixture of disparate technologies, networks, and computing systems; and people collaborating, perhaps from across the globe, who may not have ever met face-to-face. These factors make security a prime concern for organizations that conduct business online [6]. Currently, there is a profusion of online controls, for example, digital signatures, digital certificates, encryption, security protocols, virtual private networks, and so on [5]. However, a systematic conceptual approach to categorize these controls and make them understandable to managers is conspicuously absent.

The purpose of this paper is to provide frameworks for online controls using the auditing perspective of internal controls. First, this paper categorizes the online controls in the framework of COSO (Committee of Sponsoring Organizations) Report [9] and AICPA (American Institute of Certified Accountants) issued SAS (Statement on Auditing Standards) No.s 53 and 78 [1,2]. Such a categorization is beneficial to accountants and auditors. Next, a conceptual framework based on the objectives of internal controls is presented. This approach is more managerial in nature and helpful to managers who are interested in understanding the objectives behind online controls. These approaches are complementary and enable us to ask intelligent questions regarding online internal controls even if we do not have a full technical understanding of the said controls.

INTERNAL CONTROLS AND COSO FRAMEWORK

Internal controls are basically systems of checks and balances. The purpose is to keep the organization moving along the desired lines as per the wishes of the owners and to protect assets of the business. Internal controls have received attention from auditors, managers, accountants, fraud examiners, and legislatures. Internal controls are also affected by changes in business and information technology. As such, the sophistication, scope, and interpretations of internal controls have evolved over the years. However, internal controls do not have a standard definition, standard objective, and a single owner. There are two basic questions– What are internal controls? What function do they serve? The answers to these questions, of course, depend on who is answering the question.

Table 1: Perspectives on Internal Controls

ISACA	**Definition:** The policies, procedures, practices, and organizational structures are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.	**Components:** Planning and organization Acquisition and implementation Delivery and support Monitoring **Focus**: Information Technology
IIA	A system of internal controls is a set of processes, functions, activities, subsystems, and people who are grouped together or consciously segregated to ensure the effective achievement of objectives and goals.	**Components:** Control environment Manual and automated systems Control procedures **Focus**: Information Technology
COSO	A process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: • Effectiveness and efficiency of operations • Reliability of financial reporting • Compliance with applicable laws and regulations	**Components:** Control environment Risk management Control activities Information and communication Monitoring **Focus**: Overall entity
AICPA	A process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: • Reliability of financial reporting • Effectiveness and efficiency of operations • Compliance with applicable laws and regulations	**Components:** Control environment Risk management Control activities Information and communication Monitoring **Focus**: Financial Statements

Source: Colbert and Bowen [8]

The major US organizations that have articulated concepts of internal controls include ISACA (Information Systems Audit and Control Association), IIA (Institute of Internal Auditors), COSO, and AICPA [8]. These efforts are not independent but borrow from each other in an evolutionary spiral. Internal controls are viewed as an amalgam of business models, organizational processes, organizational procedures, people, and information technology. These controls are used in safeguarding assets of the business, providing relevant and reliable information, promoting operational efficiency, and complying with managerial policies and procedures.

The responsibility for instituting and maintaining internal controls rests with the management. In the real world, involvement of various layers of management in internal controls varies widely. Internal controls provide reasonable not absolute assurance. Since internal controls are subject to cost benefit analysis. All internal controls have limitations such as collusion by personnel to overcome controls, override by the top management, and human error. Internal controls ideally should evolve in tandem with the changing business conditions; thus the need for continuous management monitoring.

Each organization defines components of internal controls differently, though there are number of similarities. The components defined by COSO and adopted by the AICPA are comprehensive and are briefly discussed below in the context of online controls.

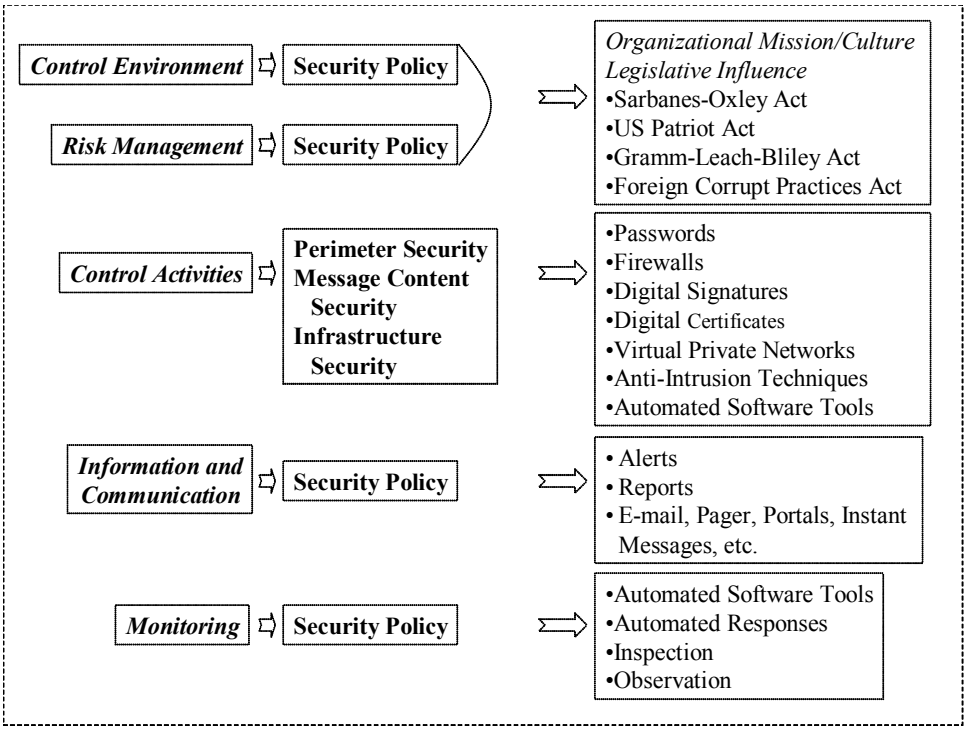

Figure 1: The COSO Framework and Online Controls

Control Environment

This is a foundation of internal controls since it deals with the people aspect. Control environment signifies attitudes of people in-charge of the organization toward the controls. The tone set at the top soon permeates the entire organization. As such; no system of internal controls is effective unless actively supported by the top management. The different elements of control environment are as follows:

- Management's commitment to integrity and ethics
- Management's philosophy and operating style
- Complexity of the organizational structure
- Oversight exercised by the board of directors, audit committee, and internal auditors
- Procedures for delegating authority and responsibility
- Human resource policies and procedures
- External influences such as the requirements of Sarbanes-Oxley Act

Risk Management

All businesses face internal and external threats. Risk analysis involves analyzing these threats and taking proactive and reactive steps to mitigate risks. The steps involved in the risk analysis are given below:

- Identify threats in the financial, operational, and strategic areas
- Estimate risks involved in each threat
- Assess cost of loss due to the risk, that is, the likelihood of occurrence of risk multiplied by possible loss
- Manage risk by designing appropriate controls
- Make sure that all controls undergo cost/benefit analysis

The online equivalent of control environment and risk management is Security Policy of the organization. The security procedures and internal controls must embody the strategic, cultural, political, and technological aspects of an organization [11]. Security policy is the place where these factors are integrated to develop a comprehensive framework for security. Security policy contains goals and objectives of the security system, defines overall purpose of the security system, and provides direction for implementation of the security system [12]. Security policy is generally designed for the entire information system, not only the online component. However, the ensuing discussion focuses on the online component of the security policy. The questions that are addressed by the security policy can be simplistically stated as follows.

- Who will use the system?
- What will be the rights and responsibilities of the users?
- How will the remote and local users access the system?
- When the system can be accessed?
- Who will decide and grant user rights?
- How the user activity is tracked and recorded?
- What disciplinary actions will be taken for errant users?
- What are the procedures for responding to security breaches?

Designing security policy is a multi-disciplinary process [7]. As the COSO report states, involvement of the top management is crucial. The senior management knowledge, operational management knowledge, information technology knowledge, and financial knowledge is required to complete the assessment required to design a security policy. The process is interdisciplinary and iterative. The designed policy is not set in stone but changes as the organization changes and need constant updating and maintenance.

Control Activities

These are policies and procedures that ensure that the management's directives are carried out. The five classes of these policies and procedures are given below.

- Appropriate authorization of transactions
- Separation of duties
- Proper design and usage of documents and records
- Safeguarding of assets and records via adequate access controls
- Independent verification, for example, internal and external audits

The online equivalent of control activities can be broken down into three categories: perimeter security, message content security, and infrastructure security. Perimeter security involves protecting the perimeter of the organizational network; however, defining perimeter of the organizational network is a tricky issue. Message content security deals with the security of the messages traveling over the Internet, intranet, and extranets. Finally, infrastructure security deals with protecting the IT infrastructure of the organization.[1] The control activities in the online world are carried out by controls such as passwords, firewalls, digital signatures, digital certificates, virtual private networks, and network anti-intrusion techniques.

Information and Communication

Internal controls should identify, capture, process, and report appropriate information, which may be financial or operational. Security policy of the organization deals with the information and communication issues. Security policy will delineate the methods of communications such as alerts, reports, e-mails, or pagers. The authority to whom such information should flow will also be specified in the Security policy.

[1] Infrastructure security is a pervasive concern and can include topics such disaster recovery planning. This paper focuses only on the online aspects of the infrastructure security.

Monitoring

Internal controls should be evaluated, periodically or continuously, to assure that they are functioning as intended by the management. The methods of evaluating internal controls depend on the type of controls being evaluated, for example, evaluating tone set at the top will be different from evaluating separation of duties. Monitoring in the online environment is generally carried out by the automated software tools and also to some extent by human inspection and observation.

CONCEPTUAL FRAMEWORK FOR INTERNAL CONTROLS IN THE ONLINE WORLD

The theoretical framework advocated by COSO fits well to the controls on the Internet. This approach maps each aspect of COSO framework to the online controls. Auditors and accountants who routinely use COSO and AICPA frameworks to categorize internal controls can benefit by application of same framework to online internal controls. Next, a conceptual framework that evaluates online internal controls in terms of their objectives is presented.

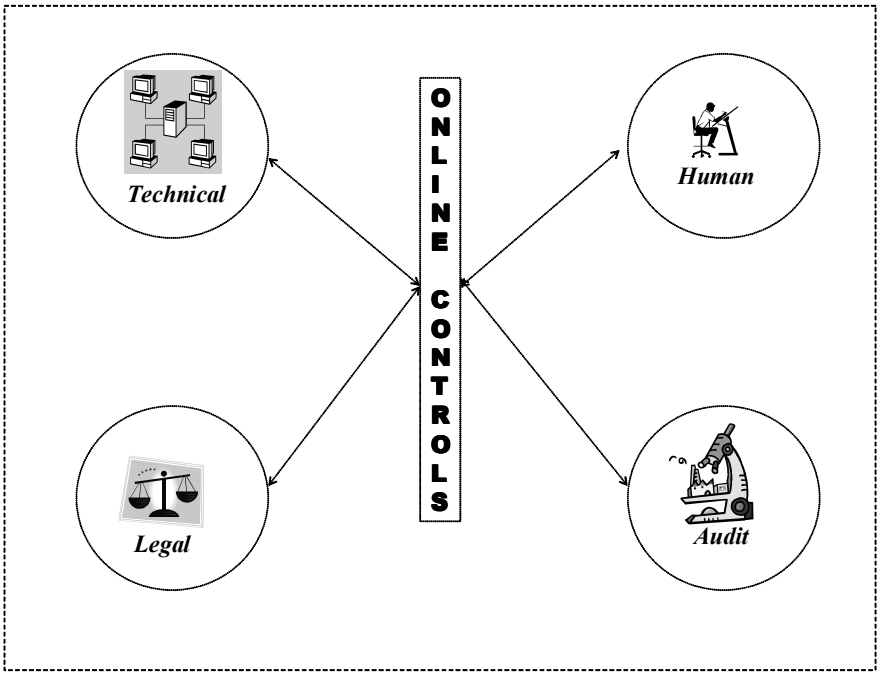

Figure 2: Dimensions of Online Controls

As shown in Figure 2, internal controls have four dimensions: technical, legal, human, and audit, which can overlap at times. Technical dimension of controls, for example, encryption has been often stressed in the control literature. The other dimensions such as audit and legal have not received much attention. This paper uses these four dimensions to forge a conceptual framework for the online controls.

The internal controls, no matter the exotic terminology, have standard objectives. The objectives of online controls can be classified as validity of transactions, mutual authentication of identity, authorization, end-to-end data integrity and confidentiality, non-repudiation, and auditability of transactions. These objectives encompass all four dimensions of internal controls as articulated in previous paragraph, and are discussed in detail in the forthcoming paragraphs. These areas are not mutually exclusive but

provide us a way to conceptually organize and discuss internal controls in the online world.[2]

Validity of Transactions

The primary question in the online transactions is the legal status of a transaction. The validity of transactions over the Internet is a legal issue. UCC (Uniform Commercial Code) a primary federal commercial law in the US, is accepted by every state, and governs the business transactions. There are numerous other commercial laws at the state level. Most of these commercial laws have been designed with paper-based transactions in mind. How do you interpret and apply these laws to the electronic transactions? This question is an important internal control issue. In general, existing commercial laws apply to e-commerce transactions. However, e-commerce also raises few novel legal issues that are not addressed by the existing laws. These issues in the online world can be stated as follows.

- Can you consider electronic records and paper documents as equivalent?
- Can you enforce the online sale if the customer denies that he/she ever placed the order?
- Are electronic agreements legally valid?
- What is the role of electronic signatures vis-à-vis pen and ink signatures?

There are three primary acts that govern the electronic transactions [4]. The first two acts, UETA (Uniform Electronic Transactions Act) and UCITA (Uniform Computer Information Transactions Act), were drafted by the National Conference of Commissioners on Uniform State Laws in 1999. The third act E-SIGN (Electronic Signatures in Global and National Commerce Act) was passed by the Congress in 2000. UETA validates electronic signatures and establishes an equivalence of electronic documents and paper-based documents. The majority of the states in the US have adopted this act. UCITA is primarily aimed at computer information transactions and applies to computer software, digital databases, digital music, and digital storage devices such as CDs and DVDs. This act in essence provides a commercial contract code for digital information transactions. The majority of the states in the US have *not* adopted this law as some of the provisions have been controversial. E-SIGN, on the other hand, is a federal statute that provides legal validity and enforceability to the electronic contracts and electronic signatures,[3] across the entire country.

Does that mean that these laws have resolved our e-commerce concerns? The answer is a qualified yes [3]. These laws in general make electronic documents and paper-based documents equivalent. The use of electronic signatures now has a legal force of paper based signatures. The electronic contracts are now legally enforceable. The electronic contracts can come in various formats, for example, in case of intangible goods such as sale of software (or rather licensing of software) there are Clickwrap, Shrinkwrap, and Boxtop licenses. The Clickwrap licenses are clickable, the types you encounter when you are installing software and the agreement pops up and will not allow you to proceed until you click *I Agree* button. Shrinkwrap licenses apply to digital products that are shrinkwraped and breaking the shrinkwrap indicates acceptance of the agreement. Boxtop licenses are generally enclosed in the boxes that contain the software or digital products. All of these contracts are enforceable. The courts have upheld these contracts as long as these agreements were consistent with the general contract principles.

The primary concerns in these areas are drafting of electronic contracts, methods of acceptance, and compliance with the letter and spirit of the law. The laws also shift the burden of proof to the corporation if the customer denies ever having ordered the goods. For such a situation, the online corporation must establish electronic controls that will enable tracing of each order to a specific customer (refereed to as non-repudiation). In the B2C transactions, the standard controls may be asking the customer for name, address, credit card number, and assigning password protected areas before the order is finalized. UETA, UCITA, and E-SIGN have rationalized conduct of the online transactions though this is an emerging legal area and not all questions are answered. Facts to be remembered as internal controls are designed for online transactions.

[2] The relationship between Figure 1 and Figure 3 is complex. The objectives of internal controls enumerated in Figure 3 cut across COSO framework. For example, the objective of data integrity and confidentiality is applicable to risk management, control activities, and information and communication in the COSO framework. This difference is due to the fact that the objectives in Figure 3 are specifically developed for controls whereas COSO framework is more general and applicable to the entire organization.

[3] E-SIGN defines electronic signature as an electronic sound, symbol, or process, attached or logically associated with the contract or other record and executed and adopted by a person with the intent to sign the record. This definition is broader than, but includes, digital signatures.

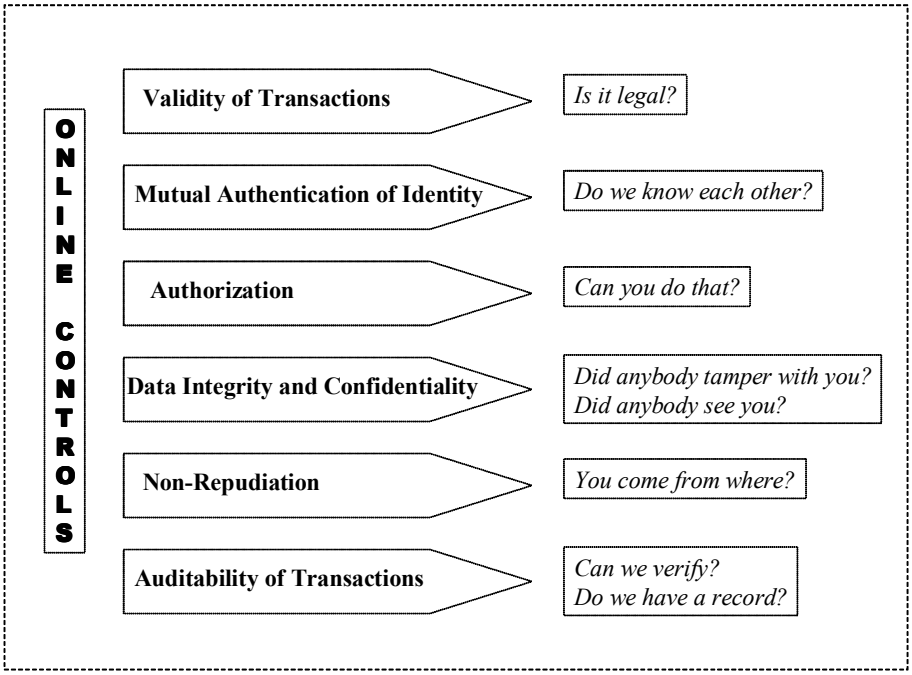

Figure 3: A Conceptual Framework for Online Controls

The USA Patriot (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001 has specific provisions to combat money laundering and financing of terrorist activities. This act is applicable to the financial institutions; and also to entities such as broker-dealers, insurance companies, credit unions, mutual funds, credit card companies, and money service bureaus. The act will eventually apply even to travel agents and car dealers. Money laundering refers to funds that were illegally acquired, generally through criminal activities, and then routed through a financial institution to make it look legitimate. The act also adds funds that are legitimately moving through the financial institutions but have ultimate purpose of financing illegal activity, to the definition of money laundering. The act requires financial institutions to detect, deter, and report all money laundering activities. The financial institutions need to watch financial transactions from money laundering perspective and should have compliance programs in place. A non-compliance with the act may result in severe civil and criminal penalties, for example, eBay's PayPal was charged with violating the provisions of US Patriot Act on March 31, 2003 by US Attorney's office. The next day, eBay's shares went down by $4 per share, a total loss of approximately $1 billion in market capitalization [10].

Another important issue on the Internet is privacy of customer information. Privacy has been an important issue for a long time; though becomes even more urgent in the online world. The Internet enables collecting, storing, analyzing, and selling of customer information very easy. Additionally, such information can be collected without the consumer's knowledge or consent. GLBA (Gramm-Leach-Bliley Act) deals with privacy issues in the context of financial industry, banks, securities firms, and insurance companies. GLBA provides guidelines for protecting customer and member information. The objectives of GLBA are to ensure security and confidentiality of the nonpublic personal information and to protect against destruction or unauthorized access of such personal information. GLBA does not provide specific guidance on how to achieve these objectives; it is left to the individual organizations. However, since GLBA deals with privacy and control issues, it must be factored in while designing internal controls. A number of automated solutions have come to the market to manage risks associated with compliance of these new laws.

.

Finally, design of internal controls should also cover auditing concerns. Internal controls in this area deal with tracking, validating, recording, and maintaining audit trails for online transactions. The storage of past transactions, backups for the storage, and easy access to the disputed past transactions are some of the areas that need to be addressed in this regard.

Audit trail needs to be maintained for valid and invalid transactions, especially if invalid transactions indicate security violation or inappropriate user activity. audit trails for online transactions. The storage of past transactions, backups for the storage, and easy access to the disputed past transactions are some of the areas that need to be addressed in this area. This is important due to the ease with which electronic records can be erased and intrusion tracks or fraudulent activity can be covered.

The personnel who handle online auditing duties need to be qualified, have clear responsibilities, and supported by the management. Technical solutions are only the first line of defense. Sarbanes-Oxley Act of 2002 mandates documentation of internal controls over financial reporting by the management. If the networks are used for financial transactions, and that is the purpose networks in business, then management needs proper understanding of controls and should be able to assess the adequacy of documentation.

Mutual Authentication of identity

Authentication is a process of verifying identities of the transacting parties. It involves determining whether someone or something is, in fact, who or what it is declared to be. Authentication of identity has two facets, one identity of the machines and identity of the humans operating the machine.

Such authentication can be carried out by means of static or dynamic passwords or PINs (personal identification numbers), passwords or PINs and security tokens, automatic callbacks, and biometric techniques. The use of digital certificates is also increasingly common. Establishing identity of a human at the end of the machine is primarily a matter of intra organizational controls. It requires review of access controls and separation of duties within the organization. The human user is identified by something the user knows, carries, or something about the user. These criteria include passwords, ID cards, or biometric measures such as fingerprints.

Authorization

Authorization is the step after authentication. The machine and user are identified and are allowed access to the computer system in the authentication phase. Then the authorization phase deals with granting rights to the user to perform certain things. These rights define types of resources and actions allowed to the user, for example, the user can read, write, or modify but cannot delete files. The rights can be assigned via ACLs (Access Control List).

Accounting, which may follow authorization, involves collecting statistics and usage information for a particular user or class of users. This information is then used for authorization control, billing, trend analysis, resource utilization, and capacity planning.

Data Integrity and Confidentiality

Data integrity refers to transfer of data without any modification, intentional or unintentional, in the transit. Data confidentiality refers to inability of the unauthorized parties to access data. The standard controls in this area include encryption, security algorithms, and communication protocols such as SSL (Secure Sockets Layer).

Non-repudiation

Non-repudiation refers to the proof that the electronic document was sent by the sender and was received by the receiver. The three aspects of non-repudiation are: non-repudiation of origin, non-repudiation of receipt, and non-repudiation of submission. Non-repudiation covers problem of the post facto denial of an electronic transaction by the transacting parties. First, it proves that the transaction took place and second, it establishes identity of the transacting parties. The controls such as digital signatures and digital certificates address non-repudiation.

Auditability of transactions

Auditability of transactions refers to the existence of audit trail and the ability to verify past transactions. The transactions should be validated, controlled, and recorded properly. A log of users, resources used by the users, and various system functions is also required for auditability. The audit trail problems can be solved by maintaining backups, time stamps, and file linkages.

The common online internal controls are classified according to the elements of the framework in Figure 4. Security policy, being the intent of the management, forms the basis for employing various controls. This classification helps in asking the right

questions. For example, internal control questions over e-mail can summarized as follows.

- How do you know that the e-mail is valid?
- How do you know e-mail came from the person identified in the e-mail?
- How do you grant permissions for users of e-mails to do e-mail related activities?
- How do you know e-mail was not altered in the process?
- How do you know that nobody has seen the e-mail?
- How can we trace earlier e-mails?

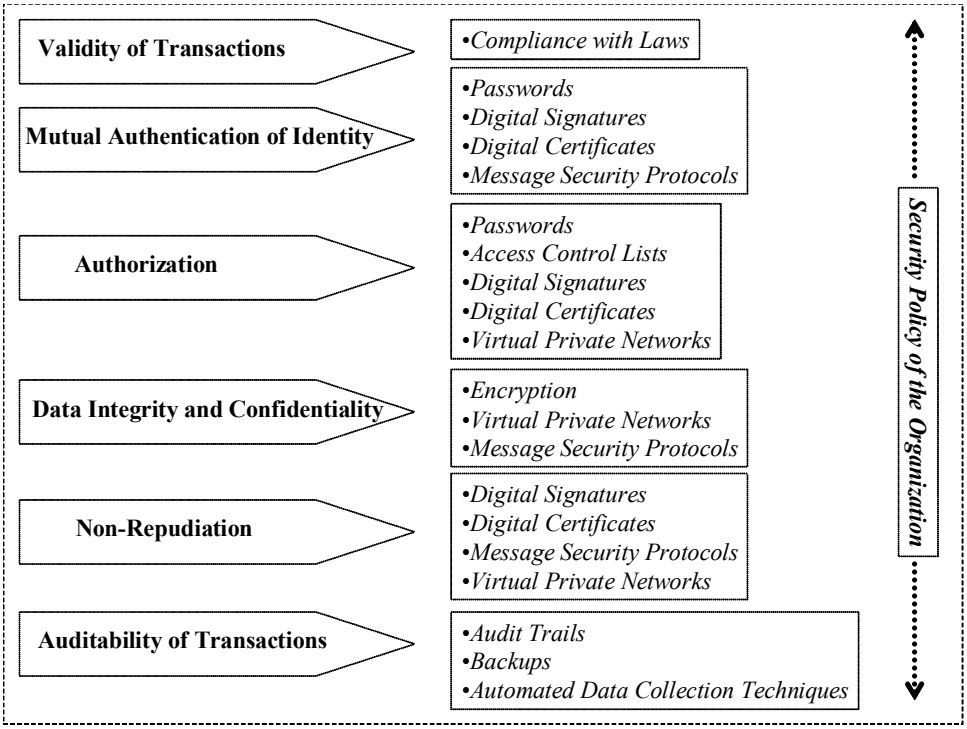

Figure 4: the conceptual framework and online controls

These questions do not need any technical understanding of the internal controls for the Internet. The framework simply enables us to ask intelligent and logical questions. These areas in the conceptual framework are not mutually exclusive and a control technique can perform several or more functions such as validity, authorization, and authentication at the same time.

CONCLUSION

A profusion of online controls has created problems in understanding purposes and objectives of online internal controls. This paper presents conceptual approaches to the online controls to aid our understanding of controls on the Internet. First, COSO/AICPA framework is presented. The online internal controls are then classified according to this framework. This classification is useful to accountants and auditors in understanding the purposes of online controls.

Next, a conceptual framework was developed based on the objectives of online internal controls. The objectives of internal controls were stated as validity of transactions, mutual authentication of identity, authorization, data integrity and confidentiality, non-repudiation, and auditability of transactions. This framework enables us to ask intelligent questions regarding internal controls even in the absence of full technical understanding of the said controls.

REFERENCES

[1] American Institute of Certified Public Accountants. Statement on Auditing Standards No. 53, The Auditor's Responsibility to Detect and Report Errors and Irregularities, New York, NY, AICPA, 1988.

[2] American Institute of Certified Public Accountants. *Statement on Auditing Standards No. 78, Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55,* New York, NY, AICPA, 1996.

[3] Baumer, D., Maffie, R., and Ward, A. "Cyberlaw and E-Commerce: An Internal Audit Perspective," Internal Auditing, November/December, Volume 17, 2001, pp. 24-31.

[4] Bernstein, G. and Campbell, C. "Electronic Contracting: The Current State of the Law and Best Practices," *Intellectual Property & Technology Law Journal*, September, Volume 14, 2002, pp. 1-11.

[5] Boncella, R. "Web Security for E-Commerce," *Communications of the Association of Information Systems*, Volume 4, November, 2000, pp. 1-43.

[6] CERT Coordination Center. "CERT/CC Overview Incident and Vulnerability Trends," *White Paper*, Software Engineering Center, Carnegie Mellon University, Pittsburgh, PA 15213, 2002.

[7] CISCO. "Network Security Policy: Best Practices White Paper," *White Paper*, http://www.cisco.com/, 2003.

[8] Colbert, J. and Bowen, P. "A Comparison of Internal Controls: COBIT, SAC, COSO, and SAS 55/78," http://www.isaca.org/Content/ContentGroups/Bookstore6/Book_Reviews/A_Comparison_of_Internal_Controls_COBIT,_SAC,_COSO_and_SAS_55_78.htm, 2004.

[9] COSO (Committee of Sponsoring Organizations). *Report of the National Commission on Fraudulent Financial Reporting*, National Commission on Fraudulent Financial Reporting, 1987.

[10] Duh, R., Jamal, K., and Sunder, S. "Control and Assurance in E-Commerce: Privacy, Security, and Integrity at eBay," *Taiwan Accounting Review*, Volume 3, Number 1, October, 2002, pp. 1-27.

[11] Sun. "How to Develop a Network Security Policy: An Overview of Networking Site Security," *White Paper*, http://www.sun.com/software/whitepapers/, 2003.

[12] Taylor, L. "Seven Elements of Highly Effective Security Policies," http://www.zdnet.com/, 2002.

AUTHOR BIOGRAPHY

Ashutosh V. Deshmukh is Associate Professor of Accounting and Information Systems at the Pennsylvania State University – Erie. His research and teaching interests are in accounting information systems and auditing. He is the author of over 20 articles in the areas of accounting information systems and auditing. He has practical experience is in public and industrial accounting. He is an Associate Editor for the *International Journal of Accounting, Auditing, and Performance Evaluation*.