Debate about Control Self-Assessment Model for e-Business System Safeguard

- e-Business 시스템 안전성확보를 위한 자가통제평가 모델에 관한 연구 -

Seo Jang Hoon *
서 장 훈

Abstract

자가통제평가(CSA : Control Self Assessment)는 핵심사업 목적을 달성하는데 개입되는 위험 그리고 그러한 사업위험을 관리하기 위하여 설계된 내부통제를 공식적이고 문서화된 협력적 프로세스에 의하여 검토하기 위하여 사용되는 방법론이다.
현재 많은 기업에서 효과적인 조직통제와 비즈니스 프로세스 개선을 위하여 전문 감사인과 경영인들이 기업지배구조 조직의 강력한 위험관리 도구로서 자가통제평가의 필요성을 강조하고 있다. 자가통제평가는 해당 조직의 담당부서나 팀에서 내부통제평가를 통하여 내부통제상의 재무보고, 준법, 사업 및 운영상의 효율성 등을 확보하기 위해서 설치되며, 효과적인 모니터 장치로서 기업지배구조상의 업무 프로세스를 정비하고 업무에서 발생하는 제반 정보의 흐름을 원활하게 해서 조직에게 손해가 발생할 수 있는 여러 가지 위험으로부터 회사를 사전에 차단하는 기능을 한다. 이러한 부분에서 효과적인 자가통제평가 시스템을 구축하는 것이 중요할 것이다.
본 연구에서는 e-Business 관련 기업지배구조의 안전성을 확보하기 위한 자가통제평가 모델에 대한 개발 필요성과 관련 자가통제평가 세가지 기본 모델들을 통하여 장단점을 제시하고, 자가통제평가 모델의 필요성을 논의하였다.
Keywords : CSA, Information System, e-Business Safeguard.

1. Introduction

CSA is a management technique that are assures stakeholders, customers and other parties that the internal control system of the business is reliable. It also ensures that employees are aware of the risks to the business and they conduct periodic proactive reviews of controals. CSA has received increased attention within

* KMAC and Ubipia Consultant
2005년 11월 접수; 2005년 12월 수정본 접수; 2005년 12월 게재 확정

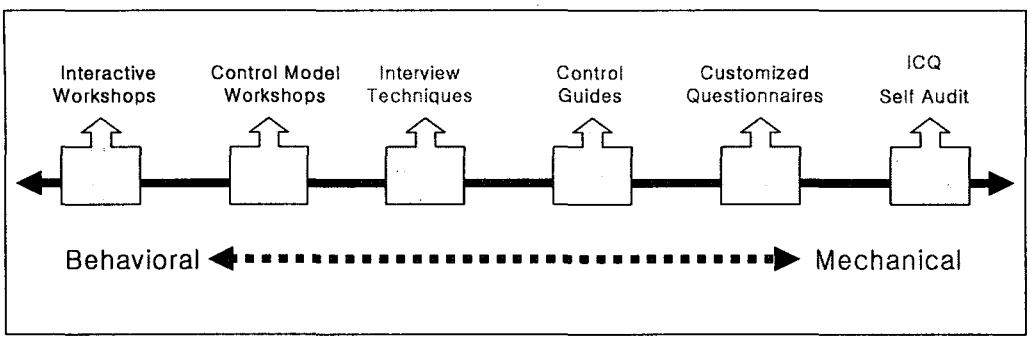
the internal audit profession during the past several years. Essentially, the technique involves bringing the staff of an entire unit(or several interrelated units) together for a facilitated workshop. Not only do they expose risk and control issues but often they devise action plans to address those issues. Today, CSA "Best Practices," like all other best practices, depend for success on the culture of the organization, the leadership of the project, and the skills of those involved. What works best in one organization may not translate well in a different environment.

CSA appears to be the right thing at the right time, for all of these reasons:

- The main impetus for choosing CSA, according to many organizations was the constraint on internal audit resources due to downsizing and budget tightening. The internal auditing department had to seek alternative methods for internal control reviews.
- CSA is an internal auditor's dream come true: management finally accepts full responsibility for internal control! Anything that fosters that kind of thinking will gain quick support among internal auditors, and internal audit has been the main advocate of CSA.
- Some implementations of CSA are collaborative and empowering-two very powerful tools that have gained a lot of support with both internal auditors and management.
- Some models of internal control and organizational development point to a process like CSA as a natural evolution of management control.
- Recent changes in legislation in several countries have placed a responsibility to report more regularly and more thoroughly on business controls.

2. Six Methods of CSA

All CSA methods generate a lot of data. Although the aggregate of data is not much more than a normal program of internal audits, the data comes in large clumps instead of being spread out over an extended audit schedule. It is important that CSA practitioners are prepared for handling large amounts of data in very short periods of time. Depending upon the CSA method chosen, there are hardware and software aids to help capture, store, manipulate, and report out the data generated by CSA.



<Figure 1.1> CSA Continuum

There are six methods for CSA in use today(refer to figure 1.1). The methods range from the most mechanical (least human contact possible) self-administered audit by Internal Control Questionnaire (ICQ) to the most behavioral (most human contact) group workshops. A lot of publicity has been given to the behavioral side of CSA, but there are CSA practitioners getting good results from methods other than group processes. FSA principles can be applied regardless of the method chosen (Various organizations are working on developing CSA models for IT-related process ; however, none has developed a generic model. In Control and Risk Self Assessment, David McNamee has described six methods):

- ICQ Self Audit
- Customized Questionnaires
- Control Guides
- Interview Techniques
- Control Model Workshops
- Interactive Workshops

2.1 ICQ Self Audit

ICQ(Internal Control Questionnaires) are commonly used by external auditors to record their understanding of internal control. The ICQ is a series of questions used by the auditor as a checklist of expected controls. The questions are about various control activities that may be or should be present in the operation. Any answer other than yes or n/a requires an explanation. The ICQ is filled out by the auditor using observation and interviews during the preliminary assessment phase of the audit. The ICQ helps determine the level of control activity and therefore the level of testing and overall scope of the audit. This tool has been brought over and used successfully in traditional ("direct report") internal auditing as part of the preliminary survey phase of the internal audit.

Some audit organizations take the ICQ and ask management to fill it out as a form of self audit. Some auditors use this technique as a completed self audit, while others use the results as a preliminary survey and risk assessment tool prior to an audit. The latter practice is to issue the document and allow 30-60 days for its return. The audit organization needs to include with the ICQ:

① Documentation to explain internal control concepts,
② The purpose of the instrument, and
③ Instructions and examples on how it should be filled out.

2.2 Customized Questionnaires

A step up from handing out Internal Control Questionnaires for self auditing is the use of customized structured questionnaires. Questions about internal controls are developed to be answered either yes or no. The questions may be customized to comply with certain regulations or laws, such as the CSA questionnaire in use at the University of Tennessee (USA). At UT, the CSA process is in addition to and separate from the internal audit process, so the questionnaire is designed to stand alone.

Another questionnaire type is used at the City of San Jose, California (USA) as an integral part of the internal audit process. The San Jose City Auditor sends out a package to all department heads scheduled for audit within 90 days of their audit date. The package is transmitted through the City Manager for emphasis. The request asks the departments to fill out a detailed questionnaire listing their primary internal controls and how the controls are monitored. Within the package sent out is a description of internal control, a step-by-step description of the audit process, and other information and instructions on how to complete the self-audit.

The City Auditor's staff receives the package back within 30 days. They then review the package for completeness before beginning the analysis on control strength in the department. During the audit fieldwork, the staff auditor will verify some of the self-audit items as a form of quality assurance.

The San Jose City Self-Audit has its roots in the Internal Control Questionnaire; however, it is that and much more. The self-audit is also a time saver in that much of what would be done by preliminary survey is completed by the department being audited. It does not involve the audit customer in designing the audit process or evaluating the controls; however, it does involve the customer in identifying the risks and controls in that part of city operations.

A third form that this process takes is the internal control sign-off, a binder of questions about various control activities that contains:

① A description of the control activity.
② A schedule when that activity must be performed (daily, weekly, monthly, quarterly, etc.).
③ A space for sign-off by the "internal control officer" (or manager) and the date signed and activities performed.

These are permanent customized questionnaires that are subject to verification by upper management and the internal auditor at any time. It is not unusual to find such binders in highly regimented control environments such as prisons and the military, or in extremely high risk areas such as nuclear power generation, casino cash handling, and pharmaceutical processing.

All of the questionnaires are removed from human interaction about the content of the questions or the veracity of the answers. Care must be taken that the questions are carefully considered and that the answers reflect the true state of affairs. One agency in New York (USA) changes the questions slightly each year to prevent receiving a photocopy of the previous year's answers. A weakness in the ICQ approach is carried over to the customized forms of questionnaire as well: In the attempt to keep the process simple, it becomes obvious that the "correct" answer is yes. This may create a certain amount of pressure to stretch the truth at times. Accumulation of data is usually quite easy because the answers are binary (yes/no), although the data can be voluminous. Questionnaires have been in use since the mid-1980s as an early form of CSA. The same FSA techniques can be used for customized questionnaires and control sign-off books as described above for ICQ Self Audit questionnaires.

2.3 Control Guides

Control Guides are binders with a description of the expected set of internal controls for the operations covered. These guides are issued by auditors and/or controllers to cover internal financial controls in operations. They are still used by internal auditors who perform mostly financial audits. In the CSA version, these control binders become Internal Control Workbooks. Internal Control Workbooks at Clorox (USA), for example, serve as essential communication links with operating management.

The example features of the Clorox Internal Control Workbooks. The workbook covers 14 Financial control areas typical of a manufacturing company. The workbook provides a list of risks related to each of the 14 financial control areas. For each risk identified, the audit staff provides a series of questions to help the audit client determine what control activities are in place to mitigate the risk at that location. The audit client makes an assessment as to how well each specific risk is controlled.

The workbook exercise is used to start a dialogue about operations, risks, and controls. Internal auditors and operations management discuss the completion of the workbook, and the completed workbook pages are sent in to internal audit for use as part of the preliminary survey. The CSA advantage, according to Clorox, is establishing a partnership with operations in the audit process, giving operations full responsibility for control specification, design and maintenance. Clorox also stated that their audit fieldwork was reduced by 40-50% per manufacturing facility.

2.4 Interview Techniques

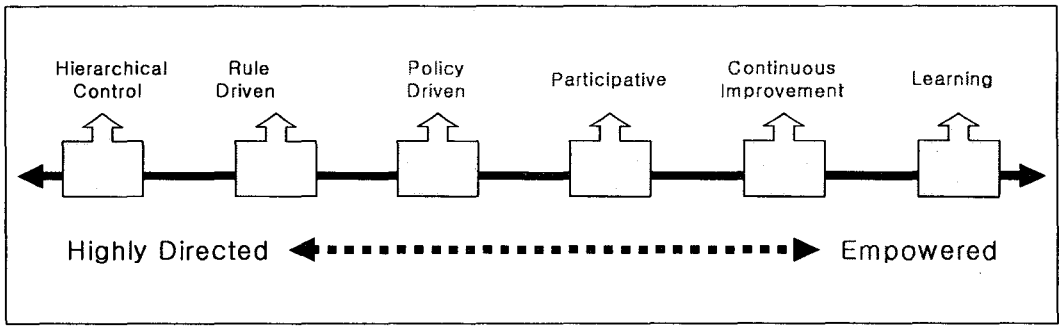
Interview Techniques One application called CSA by the practitioners is based on a series of interviews with senior management. Many internal audit departments interview or poll senior management about issues, plans, and concerns as part of the annual planning cycle. The CSA approach using the interview techniques is a more structured tool.

Bremer Financial Services (USA) is a bank holding company. They use a structured interview tool containing 57 COSO "building blocks" that is administered to a number of senior management. The tool is supplemented by an all-employee survey on ethical issues. Unlike the use of ICQ or Control Guides, the Interview Techniques approach to CSA allows for some interaction between information provider and information gatherer. This brings the two closer together in partnership rather than just a process of filling out forms and mailing them back. Using the structured interview as the basis for gathering management's input to the assessment process ensures the same questions are addressed in each session. When CSA is discussed among internal auditors, most refer to some form of work group session model that grew out of the original Gulf Resources (Canada) experience as developed by Bruce McCuaig, Paul Makosz and Tim Leech in the latter part of the 1980s. The original developers evolved two distinctly different versions of the original workshop models:

- **Control Model Workshops** : (Also known as Control Design Workshops) Training seminars that focus mostly on raising the knowledge and capability of management and staff to deal with assessing, managing, and reporting on internal control through control design models.
- **Interactive Workshops** : Process consultation workshops that focus mostly on drawing out evaluations from management and staff about the state of internal controls.

2.5 Control Model Morkshops

Control Model Workshops are championed by Tim Leech and MCS Consulting. These workshops use a purchase of information or expertise model where the central premise is that the facilitator needs to transfer knowledge to the work group in order for the work group to complete the task of assessing controls and risks(refer to figure 1.2). This approach tries to build up knowledge of assessment and design of internal control systems and the assessment of risk. Control Model Workshops focus their effort on training and control design. An example of the Control Model Workshop method: The Independent Order of Foresters (USA) uses a series of six half-day workshops. The first two are training workshops about the methods and process of CSA. The remaining four workshops deal with objectives, risks and controls.



<Figure 1.2> Corporate Culture Continuum

In the workshops, Leech does not use anonymous voting tools. He favors the use of anonymous voting tools only while collecting information about the candidness/safety of the culture. "I'm concerned that anonymous voting can send the wrong message, creating a situation in which the organization does not feel candid responses are safe." The MCS Integrated Control Frameworkis used by some Control Model Workshops. Major categories include:

① **Business/Quality Objectives** : The definition and communication of organizational goals and objectives.
② **Commitment Controls** (from the Canadian CoCo Report on Internal Controls Criteria) : Controls that involve and bind the people in the organization, such as Vision, Mission, and Purpose Statements and their influence on control and behavior.
③ **Planning and Risk Assessment Processes.**

④ **Competence/Training/Continuous Learning** : The acquisition and maintenance of the necessary skills to achieve the organization's goals.
⑤ **Direct Control Activities and Mechanisms.**
⑥ **Indicator Controls** : Performance indicators of control problems, such as fraud.
⑦ **Monitoring/Feedback** : The process of gathering and using information to adjust the control system

2.6 Interactive Workshops

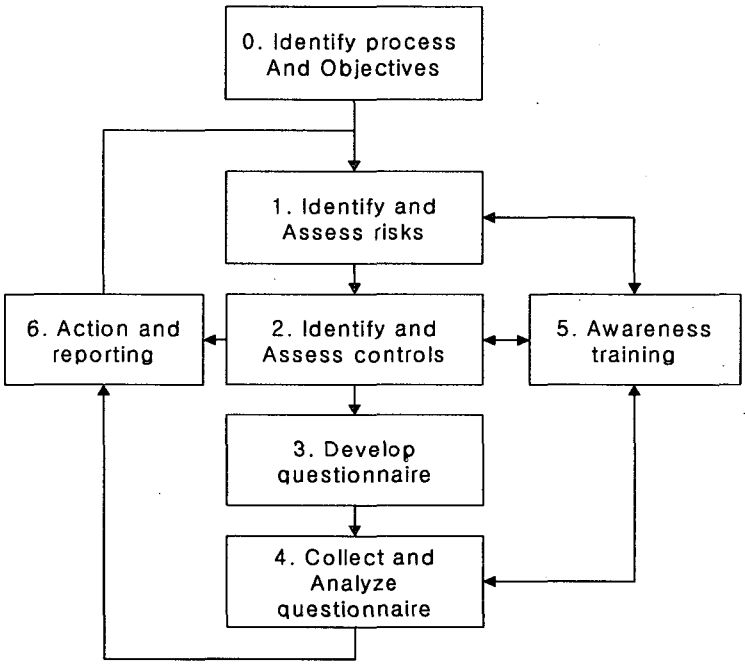
Interactive Workshops are championed by Paul Makosz of PDK Consulting. This approach uses a process consultation model (Note 17) where the central premise is that management owns the issue of internal control, and management continues to own the problem throughout the workshop. The facilitator draws out the information during the workshop. The Interactive Workshops also grew out of the original Gulf Resources (Canada) experiments. Some of the differences noted between this method and the Control Model Workshops are:

- Facilitation skills, especially in process consulting, are more necessary in the Interactive Workshops.
- Interactive Workshops are not as long because they do not emphasize the element of instruction or training.
- Anonymous voting tools are favored by the users of Interactive Workshops, but not by Control Model Workshop users.

Both use control frameworks to ensure completeness of coverage. The early Interactive Workshops of Gulf Resources used a model developed by Rod Anderson (a Canadian Accounting Professor). Interactive Workshops in other organizations have begun to use COSO or CoCo criteria, or even Malcolm Baldrige criteria.
The CSA Control Model Workshops, according to Tim Leech, should be a substitute for traditional internal audit. CSA Interactive Workshops are seen more as another product line available to the internal auditing department to serve management and the organization. CSA Interactive Workshops are seen as a supplement to traditional auditing.
Typically, each workshop lasts from a half to a full day, and each workshop is facilitated by two members of the internal audit staff: usually an audit manager and one of the audit staff assigned to that client organization. Preparation includes:

- Building trust to ensure that candor can be expressed freely.
- A strong agreement about the objectives of the process.

The workshop consists of group analysis of the strengths and weaknesses of the control systems that the department relies on to help them achieve their objectives The CSA program follows a definite life cycle. The stages of this life cycle are outlined in. [Figure 1.3] A database that can be updated is created during the first cycle- With every cycle, the CSA program matures and forms the natural business process.



<Figuare 1.3> CSA Life Cycle Stages

3. CSA Models

Three models that use one or more of the above methods are discussed in more detail below :

- NIST model : The US National Institute of Standard and Technology(NIST) developed a CSA questionnaire in September of 2001. The questinnaire can be used to develop a CSA for any organization.
- COBIT model : Developed by the IT Goverance Institute, this standard can be used to implement the internal controls on which a CSA model can be based.
- Business Process Model : EAch business process has risk of failure. CSA models are based on the identification of risks for each process and controls against materialization of the risks.

3.1 NISI Model

NIST has identified three basic controls for IT processes : Management, Operational, Technical.

Within each of the control areas are a number of topics. For example, personnel security, contingency planning and incident response are topics that can be found under the operational control area. There are a total of 17 topics (refer to table 1.1I) Each topic contains critical elements and supporting security control objectives and techniques about the system. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

<table 1.1> Topics Within control Areas

Management Controls	9. Contingency planning
1. Risk management	10. Hardware and systems software
2. Review of security controls	11. Data integrity
3. Life cycle maintenance	12. Documentation
4. Process authorization processing (certification and accreditation)	13. Security awareness, training and education
5. System security plan	14. Incident response capability
Operation Controls	Technical Controls
6. Personnel security	15. Identification and authentication
7. Physical security	16. Logical assess controls
8. Production and input/output controls	17. Audit trails

Each control objective and technique may be implemented, depending on the system and the risks associated with it. Under each control objective and technique question, one or more source documents are referenced.

To measure the progress of effectively implementing the needed security control, five levels of effectiveness are provided for each answer to the security control question:

I . Control objectives are documented in a security policy.

2. Security controls are documented as procedures.

3. Procedures have been implemented.

4. Procedures and security controls are tested and reviewed.

5 . Procedures and security controls are fully integrated into a comprehensive program.

NIST has developed a questionnaire for IT system users. The questions, which are

generic, are framed to test the level of all controls. The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. The review should consist of testing the controls, as an auditor might perform tests. For example, testing access controls can be done with a penetration test; software change controls can be tested by examining system documentation change request forms, test plans and approvals, security logs and audit trails. Supporting documentation, describing what has been tested and the results of the test, adds value to the assessment and makes the next review of the system easier. However the difference between audit and CSA is that CSA is self-audit. Also, if users are aware of the control situation they may elect to skip actual testing.

3.2 COBIT Model

COBIT was born out of a research project that addressed the need for management and control of information and related technology. It resulted in this IT governance tool that helps Organizations understand and manage the risks associated with information and IT. An organization needs information to achieve its objectives, and IT resources need to be managed by a set of naturally grouped IT processes

COBIT consist of :

1. Executive Summary
2. Framework
3. Management Guidelines
4. Control Objectives
5. Audit Guidelines
6. Implementation Tool Set

Management Guidelines provides an assessment mechanism based on the maturity models, critical success factors (CSFs), key goal indicators (KGIs) and key performance indicators (KPIs). CSFs are vital and must be completed based on the choices made 1 the maturity model, while monitoring through KPIs whether or 3t an organization will reach its goals set by the KGIs.

These measurements offer the necessary direction that management needs for IT control assessment. Control Objectives and Audit Guidelines help define and implement the control framework.

Management can place the existing level of controls over IT processes at:

0-Nonexistence : there are no controls.

1-Initial : The need for controls is recognized and ad hoc controls are in place.

2-Repeatable : Controls for repeatable processes are identified and in place but

the implementation is person-dependant rather than uniform.

3-Defined : The controls have been standardized and documented. The process owners are aware of standardized control procedures.

4-Managed : A monitoring mechanism is in place to ensure the implementation of standard controls. The feedback from this monitoring is used to improve the controls.

5-Optimized : The controls have been refined to a level of industry best practice. The feedback and monitoring mechanism is placed effectively to adapt to the changes required.

Management can plot the control level by mapping:

① Current status in the organization

② Current best practices in the industry

③International best practices

④Improvement strategy

In its Board Briefing on IT Governance, 2nd Edition the ITGI provides a checklist for top management. This checklist is an; excellent tool for self-assessment to evaluate IT governance. This checklist forms the initial input for the development of CSA. The control framework of COBIT defines a set of 34 high-level IT processes with objectives for controlling the processes, which are grouped into four domains:

1. Plan and organize
2. Acquire and implement
3. Deliver and support
4. Monitor and evaluate

3.3 Business Process model

This model is based on the identification of risks associated with each business process. A process is a structured, measured set of activities designed to produce a required or specified output. The COSO generic business model forms the basis for this approach.

For effective completion of a process, controls are required to be in place. Every process has a purpose or objectives, and inputs and outputs. It also has a risk of objectives not being met. Analysis of possible threats that can cause failure in the process forms the basis for controls over the process. The controls may reduce the probability of an event occurring, or mitigate the impact of these threats if materialized. The objective of CSA is to generate a comprehensive risk and control profile. The basis for development of this model is top-down analysis of processes.

Some IT processes are a pan of a more general business process, and others are self-contained. The major IT processes of the organization may be progressively broken down into smaller tasks.

For example, starting computer operations at a computerized branch is part of the major branch operations process, which can be comprised of many smaller processes, such as checking main switches for power, checking UPS for proper output, starting peripherals, checking server power, checking power to all nodes, starting Day Begin" operations, and checking logs of Day Begin operations. Each of the smaller processes can have various obstacles and/or threats, which can stop the process from successful completion(e.g.,,load shedding might have drain6d the UPS batteries, or the Day Begin,, process may have terminated abnormally). In such situations, controls to prevent, detect and correct these situations are activated. However, the changing environment requires constant evaluation of these controls for their effectiveness. Hence, evaluation of controls is necessary to make adjustments- Periodic IS audit can aid in identifying the required changes in controls, but the effectiveness of the audit process depends on factors such as the rate of change in environment, auditor attitude, and the attitude of employees towards audit. The purpose of the CSA program is to involve process owners in identifying the need for and implementing the changed controls.

4. Need for IT-Governance Internal Controls

There are number of reasons for the use of internal controls:

① Changing business process-Developments in information and related technology over the last 40 years have made it increasingly evident to managers, controllers, regulators, government authorities, lawmakers, users and service providers that there is a need for a reference framework for security and control in IT. Effective IT management is critically important to the success of an organization, due to:

- The increasing dependence on information systems
- The increasing vulnerabilities and cyberthreats
- The scale and cost of current and future investments in IT
- The potential for technologies to change the business processes, procedures and practices of an organization

② Change of focus on IT-Organizations, particularly service sector organizations, are increasingly dependent on information technology. Organizations are also creating new IT-enabled products and services, and technocrats are predicting that future organizations will exist only in cyberspace.

③ Control investment-To maintain a successful organization, understanding and managing the risks associated with implementing new technology is essential, and to provide effective direction and adequate controls, management should have an appreciation for and a basic understanding of the risks and constraints of IT.

④ Competition-Global competition is here. Organizations are restructuring to streamline operations, take advantage of the advances in IT and improve their competitive position. Business reengineering, right-sizing, outsourcing, empowerment, flattened organizations and distributed processing are all changes that impact the way in which business and governmental organizations opeerate. These changes are having, and will continue to have, profound implications for the management and operational control structures within organizations.

⑤ Nature of business-The administrative structure of banks is based on a decentralized model and this branch office structure is applicable to many organizations. The administrator, responsible for the accomplishment of a branch's goals and objectives, is also responsible for the establishment, maintenance and monitoring of the internal control system, which helps ensure the accomplishment of goals and objectives.

⑥ Sarbanes-Oxley Act-This US Act has redefined the rules for corporate governance, disclosure and reporting.

⑦ Control self-assessment-While internal and statutory audits assist management in evaluating procedures and internal controls, auditors are unable to visit and work with each branch/office on a regular basis. To assist management in evaluating internal controls and increase the employees' understanding of those controls, CSA needs to be developed and implemented. Many organizations have considered implementation of CSA because of the constraints on internal audit resources due to downsizing and budget tightening.

5. The Need for CSA

CSA is an extension of the internal control mechanism. Unless internal controls are implemented, it cannot function. Therefore, an understanding of internal control is required. Technology adoption has expanded concern about internal controls from simply being confined to accounting functions to encompassing the entire business enterprise. In the US, increased attention to controls began in the 1970s with the

passage of the Foreign Corrupt Practices Act of 1977 and later with the Treadway Commission on Fraudlent Financial Reporting in 1987. More recently, the Federal Deposit Insurance Improvement Act(FDIIA) of 1991 and the Federal Sentencing Guidelines of 1991 have also piqued interest in understanding and applying internal control concepts.

In 1992, the Committee of Sponsoring Organizations(COSO) of the Treadway Commission published a report that established a generally accepted of internal control. This new and comprehensive framework marked a US standard for implementation and evaluation of business controls. Control Objectives for Information and related Technology(COBIT), published by the IT Governance Institute, followed and continues to refind these controls.

The 2002 Sarbanes-Oxley Act has added new dimensions to internal controls. Though the act was primarily passed to protect investors' interest, it has direct implications on internal controls of organizations. According to the Act, CEOs and CFOs must personally certify that they are responsible for disclosure controls and procedures. Each quarterly filing must contain a certification that they have **performed an evaluation of the design and effectiveness of these controls.** The certification must also state that they have disclosed to their audit committee and independent auditor any significant control deficiencies, material weaknesses and fraudulent acts.

It also mandates an **annual evaluation of internal controls and procedures** for financial reporting. In addition, the company's internal auditor must issue a separate report that attests to management's assertion on the effectiveness of internal controls and procedures for financial reporting. This last requirement necessitates the adoption of a control framework against which the internal controls can measured.

For example, the COBIT framework:

Helps management to ensure that its IT decisions balance risks and controls

Helps users obtain assurance on security and controls of the products and services they acquire

Helps auditors provide a tool for apprising management of the internal controls that exist, form opinions on internal controls for management and identify the minimum cost-beneficial controls necessary for the organization

Other documents were developed in Canada, the Criteria of Control Committee(CoCo) document, and in the UK, the Cadbury Report.

Internal control is defined by COSO as:

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

COSO also identified five components of internal control that support the achievement of the separate, but overlapping, operational, financial reporting and compliance objectives.
The enhancement of internal controls requires strengthening the internal audit function.
CSA is a tool designed to assist in the internal audit function, and to test the effectiveness of internal controls. A concise definition of CSA is not available; however, many organizations have described CSA in the following ways:
CSA is a risk management program in which risks and controls are examined and assessed to provide reasonable assurance to management that its business objectives will be achieved. The responsibility of the CSA program is shared among all employees.
CSA is a self-assessment conducted on a system (major application or general support system), or a set of multiple self-assessments conducted for a group of interconnected systems (internal or external to the organization). It is one method used to measure IT security assurance, which is the degree of confidence one has that the managerial, technical and operation security measures work as intended to protect the system and the information it processes.
CSA asks employees and managers who are directly involved in a business activity to determine whether the processes in place are effective and the objectives are being achieved.
CSA is a powerful tool because it is inclusive and sets an expectation of high performance and a high level of knowledge about the work structure and policies. CSA helps evaluate informal or subjective controls in such human resource policies. By employees' involvement of all levels, CSA solicits open communication and teamwork, and encourages improvement.
From the senior management perspective, CSA assists in determining whether the organization is meeting its objective. Key advantages to implementing a CSA program include early detection of risk and development of concrete action plans that safeguard
organizational programs against significant business risk.

The CSA goals are to:
-Reduce or eliminate costly and ineffective controls while creating valuable alternatives
-Pinpoint risk areas while developing adequate control measures

-Evaluate the control standards that are already in place
-Emphasize management's responsibility for developing and monitoring effective internal control systems
-Communicate the results to others

CSA is a technique that involves bringing the staff members together for a facilitated workshop where they can discuss risk and control issue device action plans to address those issue. The process offers a means of identifying control problems and recommendations for improvement. The facilitator helps the group reach agreement.

Self-assessments provide a method for employees and management to determine the current status of their information security programs and, if necessaary, establish a target for improvement. The method utilizes specific control objectives and techniques in which an unclassified system, or group of interconnected systems, can be tested and measured. It may not, however, establish new security requirements. The control objectives and techniques are abstracted from an organization's statute, policy and guidance on security.

CSA is a natural response to relevance that has been lost in the more traditional forms of assurance. The disconnect between those who provide audit services and their client community remains fairly severe to this day. Self-techniques are a means by which internal control owners are taking back primary ownership of assurance

To become or remain relevant to internal control owners, the audit function must transition to an integral component of the internal control process rather than maintaining the role as corporate monitor or policeman. CSA is the path to regaining relevance in an organization.

The goal is not to practice forms of audit function, but rather transition to various forms of CSA which are embedded into the routine practices of each business process, with ownership of assurance assigned to the internal control owners as part of organizational design.

The basis characteristics of CSA follow:

- It is a technique.
- It involves employees and process owners.
- The aim is to ensure that business objectives are achieved.
- It reduces the audit function load.
- It is proactive verification of internal controls.
- It increases the frequency of controls verification.
- It involves control improvement-the timely detection and correction of weak controls.

5.1 The Benefits of CSA

The benefits of effectively conducted CSA include:
① Early detection of risks
② More effective and improved internal controls
③ Creation of cohesive teams through employee involvement
④ Increased employee awareness of organizational objectives and knowledge of risk and internal controls
⑤ Increased communication between operational and top management
⑥ Highly motivated employees
⑦ Improved audit rating process
⑧ Reduction in control cost
⑨ Assurance provided to stakeholders and customers
⑩ Necessary assurance given to top management about the adequacy of internal controls, as required by the US Sarbanes-Oxley Act

5.2 Disadvantages of CSA

CSA can hold some disadvantages as well. They include:
- It could be mistaken as an function replacement.
- It is regarded as an additional workload-one more report to be submitted to management.
- Failure to act on improvement suggestions could damage employee morale.

6. Conclusion

CSA, like any other audit process, can be more useful if it is not limited to the past and present state of risk and control. By incorporating techniques to imagine the future, self-assessment tools can be used to improve business processes as well as evaluate them. By facilitating improvement, the internal auditor adds immense value to the organization. and Success of CSA depends on the culture of the organization, the leadership of the project and the skills of those involved. What works best in one organization may not translate well to a different environment. IT governance is becoming an important consideration for all organizations. CSA is an effective tool for successful implementation of IT governance. Considering the security incidences, limited internal audit resources and requirements of the Sarbanes-Oxley Act, CSA will help medium and large organizations build security consciousness among IT users and will provide a mechanism to comply with the Acts provisions.

7. REFERENCES

[1] Makosz, Paul and B. W. McCuaig, Ripe for a Renaissance, Internal Auditor, December 1990.
[2] Jordan, Glenda S., Control Self-Assessment: Making the Choice, Altamonte Springs, FL: Institute of Internal Auditors, 1995, p. 88.
[3] Cottrell, David M., et al., Continuous Improvement at Clorox, Internal Auditor, February 1995.
[4] Financial Executives Institute, COSO Self-Assessment Framework (Software), Altamonte Springs, FL: IIA (407-830-7600 X1), 1994.
[5] White, David, Directions in Internal Control, IIA South Pacific Regional Conference, May 1995.
[6] 2New Zealand State Services Commission, Report on Self Review in the New Zealand Public Sector (2 Vols.), Wellington, NZ: State Services Commission, 1992.

저 자 소 개

서 장 훈 : 명지대학교 산업공학박사, 아주대 경영대학원 MBA, 현재 Ubipia SI 사업부 수석컨설턴트, 한국능률협회컨설팅(KMAC) 컨설턴트, 관심분야는 e-Biz BPM, 6시그마, IT 프로세스 평가, 정보시스템 감사, 정보시스템 품질, 정보생산성