EVALUATING AND DESIGNING AN INTERNAL CONTROL SYSTEM FOR INFORMATION SYSTEMS USING CONTROL SELF-ASSESSMENT METHOD, 2014

TUĞBA YILDIRIM

BOĞAZİÇİ UNIVERSITY

2014

EVALUATING AND DESIGNING AN INTERNAL CONTROL SYSTEM FOR INFORMATION SYSTEMS USING CONTROL SELF-ASSESSMENT, 2014

Thesis submitted to the

Institute for Graduate Studies in the Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

In

Management of Information

Systems

by

Tuğba Yıldırım

Boğaziçi University

2014

Thesis Abstract

Tuğba Yıldırım, “Evaluating and Designing an Internal Control System for Information Systems Processes Using Control Self-Assessment, 2014”

Information systems take its crucial role in the heart of business life today. Most of the business operations are held via information technology. Achievement of business objectives are strictly related with information systems (IS) internal control system in order to create effective and efficient business processes.

It is very important for organizations to prevent undesirable events and operate activities effectively and efficiently in achieving business objectives. Fraud events took place in some of reputable organizations and the reasons for these events are concluded to be the lack of risk management and effective internal control system. After these fraudulent events in organizations, frameworks developed to manage risks and reconstruct their internal control systems. Designing an effective risk management and an internal control system is proposed as a solution for more effective and efficient operations. Recently, information systems became very important in operational activities since most of them are done by information technology. This dependency forced organizations to manage risks related with information systems and establish an IS internal control system.

Control objectives for minimizing risks, their control practices and test steps of these controls are provided in reference guides. Control objectives are located under the IS processes. Risk and control specialists deal with risks in these processes and controls to minimize them. They are expected to work on making organizations compliant with related laws and regulations as well as internal policies and rules by designing controls.

Several information can be found about importance of complying with the standards, frameworks, IS internal control system, control objectives, control practices. However, studies lack the answer for “How” to design internal control system in compliance with related frameworks and standards.

This thesis provides an answer for the question of “How to design IS internal control system?” In this study “Control Self-Assessment Method” is proposed as an effective method by mentioning essential critical IS processes.

Control Self-Assessment method is selected since it provides a flexible solution which is especially appropriate for designing an internal control system to achieve changing objectives of the companies.

Tez Özeti

Tuğba Yıldırım, “ Bilgi Sistemleri Süreçleri için İç Kontrol Sisteminin Kontrol Özdeğerlendirme Metodu ile Değerlendirilmesi ve Tasarlanması, 2014”

Günümüzde Bilgi Sistemleri iş dünyasının kalbinde vazgeçilmez bir rol oynamaktadır. Birçok iş bilgi teknolojileri vasıtasıyla gerçekleştirilmektedir. Etkin ve verimli iş süreçleri oluşturarak iş hedeflerine ulaşılması bilgi sistemleri kontrol sistemi ile sıkı sıkıya bağlıdır. Kurumlar bu hedeflere ulaşmak için en iyi uygulamaları içeren çerçeve ve standartları kullanmaktadır.

Kurumlarda; istenmeyen olayların ve kayıpların önlenmesi, operasyonların etkin ve verimli bir şekilde yürütülmesinin sağlanması büyük önem taşımaktadır. Geçmişte çeşitli büyük kurumlarda yaşanan vakaların sebebi olarak kurumlarda etkin bir risk yönetiminin yapılamaması ve etkin bir iç kontrol sisteminin eksikliği gösterilmektedir. Kurumların etkin bir risk yönetimi ile riskleri minimize edecek etkin bir iç kontrol sisteminin tasarlanması hem bu türden olayların yaşanmaması hem de operasyonların daha etkin, verimli ve uyumlu şekilde yürütülmesi için çözüm olarak sunulmaktadır.

En iyi uygulamalara ilişkin standart ve çerçevelere uyumun önemi, bilgi sistemleri kontrol sistemi, kontrol hedefleri, kontrol uygulamaları konularında çoğu bilgi mevcuttur. Fakat tüm bu bilgileri bilgi sistemleri kontrol sisteminin tasarlanmasına yönelik olarak bir arada ele alan bir çalışma olması bakımından çalışmamız önem taşımaktadır.

Bilgi Sistemleri için kontrol sistemi tasarımı, en iyi uygulamalara yönelik standart ve çerçevelere uyum konuları üzerinde çeşitli çalışmalar olmasına rağmen ilgili çerçeve veya standartlara uyumlu bir kontrol sisteminin “Nasıl” tasarlanacağı hususu açıkta kalmıştır.

Bu tez çalışması “Bilgi Sistemleri için İç Kontrol Sistemi Nasıl Tasarlanır?” sorusuna cevap sunmayı amaçlamaktadır. Bu çalışmamızı temel kritik bilgi sistemleri süreçlerine değinerek Kontrol Öz değerlendirme Metodunu uyumluluk için etkin bir araç olarak sunmaktayız.

Bu tez çalışmasında kritik bilgi sistemleri süreçleri için iç kontrol sisteminin Kontrol Öz değerlendirme metodu ile ‘Nasıl’ tasarlanacağının açıklığa kavuşturulması hedeflenmektedir.

ACKNOWLEDGEMENTS

I feel responsible to declare my appreciation to my academic advisor Assoc. Prof. Zuhal TANRIKULU and my thesis advisor Dr. Bilgin METİN for their precious knowledge supporting me in preparing my thesis.

I owe very special thanks to my dear boss Mahmut YALÇIN who always encouraged me in writing my thesis.

I am grateful to my beloved father Tacettin ÖZKAN and my mother Mediha ÖZKAN who have a great role in my life and who made me realize the significance of reading, learning and working.

Finally, I dedicate my thesis to my husband Hakan YILDIRIM who never stopped supporting me by both socially and academically during my study.

CONTENTS

FIGURES

TABLES

CHAPTER 1

INTRODUCTION

Business organizations, dealing with rapidly changing competitive industry environments, changing customer priorities and demands, are required to manage risks related with objectives and establish a reliable internal control system. In Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM, 2004) framework, it is stated that "The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders." This can be achieved by an effective risk management which enables organizations to manage uncertainty and helps management in dealing with uncertainty and asses risk and opportunity to enhance value for business and internal control system in organizations.

In Chapter 1 "Need of a Holistic Approach for Designing IS Internal Control System", a necessity for a holistic approach for designing an organization's internal control system for Information systems is discussed. Since Information Systems (IS) take its crucial role in the heart of business life and most of the businesses operations are held via information technology, achievement of business objectives are strictly related with IS internal control system. Since information technology (IT) develops with a rapid acceleration, management of internal control system for IT became more difficult. New developments bring new risks and threats to organizations to be managed. In this chapter the importance of designing and evaluating IS internal control system is stressed and apparent frameworks, standards and approaches are discussed. By looking at these resources the answer for the question of "How to design an IS control system?" is questioned and the need for a holistic approach in designing an effective IS internal control

system is stated. The importance of processes on internal control systems design and evaluation is also stressed in this chapter.

In Chapter 2, “Convenient Quality for IT -Governance- Aware Companies”, importance of quality management by an internal control system point is given. It is very important for an internal control system that policies, standards, procedures and processes are established, documented and followed. The role of quality management specialists and risk and control specialists is given. The common parts of IS quality management and internal control system is stressed.

IT Governance framework which is regarded as an effective framework to provide IT excellence and quality (Robinson, 2005) and ISO 9001:2008 can be considered together by focusing on their similar aspects, thereby increasing the quality of IT processes integrated with QMS. ISO 9001:2008 creates much more efficient and effective operation; increases customer satisfaction; reduces the number of audits; enhances marketing; improves employee motivation, awareness and morale; promotes international trade; increases profit; reduces waste; and increases productivity (Rohitratana, 2000).

In Chapter 3, “Internal Control Design for Information Systems with Control Self-Assessment Method”, Information Systems control frameworks and standards and related reference guides are taken into consideration and a concrete method for designing IS internal control system is questioned. Control Self-Assessment method is discussed for IS internal control system design since being aware of the significance of IS internal control system and rapidly changing risks and opportunities IS poses to organizations; design of this system ranks higher points in importance.

This study aims to open a door for risk and control specialists by giving a holistic approach for designing IS internal control system. By using numerous information about

characteristics of best control practices and widely accepted standards and frameworks, a method is needed for IS internal control system design. In the literature some methods are proposed for control system design and evaluation; one of which is Control Self-Assessment (CSA).

In Chapter 4, Practical Application of CSA, a practical method for risk and control professionals in helping them to assess the effectiveness, efficiency of internal control system and to provide an appropriate platform for designing internal control system; application of Control Self-Assessment method is discussed in this chapter. Different forms of CSA are defined and rules for selecting the right approach is given. Critical success factors for CSA are stated which are keys to get the best performance of CSA.

Although information can be found in academic studies and reference guides about Control Self-Assessment Method; it still lacks a practical way of implementation.

In this chapter a CSA workshop process is given in order to provide a practical way for risk and control specialists. A focus group study is made to assess the appropriateness and applicability of this process. Nine professionals attended the focus group study with an experience of 3 to 23 years with an average of 11,88 years; coming mostly from banking, information systems and consultancy sectors. All of the nine participants have at least one certification in risk, control, security, audit and governance areas. Focus group participants have 19 certificates in total. The necessity and priority of the process steps are assessed according to focus group study results.

IS internal control system is a very important enabler of an organization because most business operations are strictly related to information technology. Critical information systems processes are given in Chapter 5 “Critical Information Systems Processes” to provide most risky Information Systems processes taking generally accepted

IS standards' and frameworks' common parts. Making a risk assessment which provides a prioritization in designing internal control system by using Control Self-Assessment for these processes is recommended in this chapter.

Realizing the importance of design and evaluation of IS internal control system in achievement of business objectives, taking quality as a key step for effectiveness and efficiency of internal control system and following widely accepted governance and control frameworks with best practices, Control Self-Assessment method is recommended in this study and a practical process is given as an implementation guide. For prioritization of CSA efforts, critical processes for an IS environment is also provided in this study.

CHAPTER 2

NEED OF A HOLISTIC APPROACH FOR DESIGNING IS INTERNAL CONTROL SYSTEM

Introduction

Business organizations, dealing with rapidly changing competitive industry environments, changing customer priorities and demands, are required to manage risks related with objectives and establish a reliable internal control system. In Committee of Sponsoring Organizations Enterprise Risk Management framework, it is stated that "The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders." (COSO ERM, 2004) Undesirable past events such as in the Enron (accounting fraud, keeping huge depts off the balance sheets) and Worldcom (accounting fraud, underreported line costs by capitalizing rather than expensing, and inflated revenues with fake accounting entries) indicated again that there is a significant requirement for an effective risk management and internal control system in organizations.

In order not to face with these undesirable events and achieve business objectives with a reliable and an effective internal control system; a holistic approach is needed.

In this document, definition and importance of internal control is given, importance of quality for internal control system is stated. Objective, risk and control relationship and their importance in designing internal control system is described. Evaluation of sufficiency of apparent guidance on internal control system design is clarified by taking best practices and frameworks into consideration.

What is Internal Control?

Internal control is defined as follows:

> Internal control is defined as a process, affected by an entity's people, designed to accomplish specified objectives. The definition is broad, encompassing all aspects of controlling a business, yet facilitates a directed focus on specific objectives. Internal control consists of five interrelated components, which are inherent in the way management runs the enterprise. The components are linked, and serve as criteria for determining whether the system is effective. (COSO ERM, 2004)

Business organizations face with uncertainty to achieve business objectives and gain value for company. It is a challenge for management to determine how much uncertainty to accept in order to gain stakeholder value. "Uncertainty presents both risk and opportunity, with the potential to erode or enhance value." (COSO Executive Summary, 2012)

Establishing an enterprise risk management enables organizations to manage uncertainty and helps management in dealing with uncertainty and asses risk and opportunity to enhance value for business. In another words, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way. (COSO ERM, 2004)

Importance of Quality for Internal Control System

Wallace, in her Internal Controls Guide book claims that "Hand-in-hand with continued improvement is the notion of the quality" (Wallace, 2005). This is also the same for internal control. A widely applied Deming (who is known as the "Father of Quality") improvement cycle, Plan-Do-Check-Action (PDCA) reflects management's commitment for enhancing quality. By looking from the internal control point; two approaches have a lot in common since both are aimed at achieving business objectives, focus on identifying planned accomplishments, fulfill the planned tasks, check whether the planned are done or not and answer the question of learned lessons.

As indicated in Wallace's book, "a clear one-to-one mapping of critical aspects coherent control framework exists between the PDCA cycle and a control structure for an entity." (Wallace, 2005). Frameworks and standards are also said to improve quality management system. For example, in several publications, COBIT is regarded to be an effective framework to provide IT excellence and quality. In the "IT Excellence starts with governance" (Robinson, 2005), it is said that IT governance provides the essential bedrock for effective acquisition and deployment of technology. Another study uses COBIT to refine IT Processes for quality. In the article, refining IT processes is claimed to provide greater IT process and product quality and increased IT process efficiency and effectiveness. (Reingold, 2005)

It is very important for an internal control system that policies, standards, procedures and processes are established, documented and followed. In practice, quality management departments are responsible for consulting in process development in order to

create effective and efficient processes. Changes to these quality documents are also made by following quality management process.

While quality management specialists try to develop effective and efficient processes and quality documents for business operations, risk and control specialists concentrate on objectives, risks of these working styles and try to design controls. This is very crucial in gaining value for business without any losses.

Objective, Risk and Control Relationship

Objectives, risks and controls are strictly related to each other. In order to talk about controls there should be an objective determined by management, a risk that is related to the objective and the control which can minimize that risk in achievement of that objective.

In past, controls are regarded to be only the concern of auditors. However; controls are everyone's responsibility in an effective internal control system. (McKeever, 2009)"Controls are not special things; they are just the things people do in their jobs." (Hubbard, 2005) Controls are inseparable parts of the business. While control responsibility is everyone's; top management has an important role of "setting the tone" for their organization by fostering a control environment and they are "charged with overseeing the establishment, administration and evaluation of the processes of risk management and control" (Hubbard, 2005)

Risks are undesirable events which have a negative impact. They "can prevent value creation or erode existing value." (COSO ERM, 2004) By designing controls; risks can be minimized and maximum value can be gained.

Objectives: Things an organization wants to accomplish

Risks : Things that might prevent accomplishing an objective

Controls : Things that help meet an objective by managing that risk

Internal Control System Design

An effective control system provides reasonable assurance for safeguarding assets, the reliability of financial information, and compliance with laws and regulation. “Control system does not provide absolute assurance since it is the management’s responsibility to determine the balance between risk of a certain business practice and the level of control required to ensure whether the business objectives are met.” (Understanding Internal Controls) “Sometimes the cost of a control may be more costly than the exposed risk or than the benefit. Management and control system designers should be aware of that “The cost of a control should not exceed the benefit to be derived from it.” (Understanding Internal Controls)

When designing internal controls; the first step should be identifying the objective. After the management’s determined objective is identified, then the risks for that objective should be assessed. Management has the responsibility to response to the risks. Types of risk responses that management can decide are risk avoidance, reduction, sharing, and acceptance. (COSO ERM, 2004) If the risk is not accepted than controls should be designed by business owners and risk and control specialists.

Importance of Information Technology In Internal Control System

Information Technology, as an important enabler for business operations, brings lots of opportunities for business life such as automating processes, decreasing human error and effort and helping in decision making for management. However, it also brings lots of risks to be managed in order to enhance value and prevent undesirable events. According to Yong, "Information technology not only brings great convenience to the enterprises, but also creates numerous unsafe factors; the increasing complexity of information technology has become a major risk what the enterprise facing." (Yong, 2010)

Internal control system for information technology became crucial with increasing dependence on its effect of business. Since IT develops with a rapid acceleration, management of internal control system for IT became more difficult. New developments bring new risks and threats to organizations to be managed. Chen claims that IT changed the management pattern and increased their operating efficiency and gave a competitive advantage to the enterprises. He also refers to pretends IT as a double-edge sword, because IT increases the risk of enterprises along with bringing enterprises the results such as the govern risk of IS, the leaking risk of internal control of software, the instability risk of running system, the man-made risk etc. (Zhibin, 2007)

Debreceny stated that "The importance of designing, building, and assessing the quality of internal controls on the lifecycle of information technology (IT) investment has been heightened since the passing of the Sarbanes-Oxley Act." (Debreceny, 2006)Sarbanes

Oxley Act 2002 is the result of corporate frauds and failures of the early 2000's and this act has brought the nature and effectiveness of internal controls into focus.

Need of A Holistic Approach for Designing IS Control System

Establishment for an IS internal control system, designing controls to minimize risks, making business operations effective, efficient and also compliant with related laws and regulations and creating reliable financial reporting issues are stressed on both internal control, risk management frameworks and control focused IT governance frameworks and standards.

For example, COSO ERM framework includes details about the components of an internal control system by definitions. Furthermore, as an example, COBIT framework includes control focused objectives for IS processes. ISACA provide "Control Practices" for information systems processes. ISACA also published an "IT Assurance Guide" for auditors explaining the test steps for testing the compliance with COBIT framework. However, a holistic approach for establishing and designing an IS internal control system is not provided for risk and control professionals. Some clues are given in COBIT about methods to use in the evaluation of internal control. However, it lacks the answer for "how" to design an IS control system, although it mentions about components of a control system such as control objectives, risk drivers and value drivers for IS processes.

The information about "what to" do is given in studies, however this topic needs to be studied since it does not answer the question of "How to" design IS control system.

There still a necessity for a holistic approach defining and explaining design process of an IS internal control system.

Impact of Frameworks and Standards on IS Internal Control

Frameworks and standards are developed for effective IT governance (among them) some of which are focused on control such as Control Objectives for Information and Related Technology (COBIT). From control point of view, complying with these frameworks, standards and best practices became a facilitator for making effective, efficient and compliant IT environment and processes. This compliance also serves for the establishment and maintenance of the IS internal control system. According to O'Donnell and Rechtman (2005), COBIT represents a comprehensive set of control processes, objectives, and activities that can be customized to an entity's needs. They claim that COBIT's scalability and comprehensiveness serves an entity's complete IT needs such as designing, implementing, or reviewing them. "The systematic manner in which COBIT can be presented and used creates the opportunity to deliver an efficient and effective consulting engagement." (J.B. O'Donnell & Y. Rechtman, 2005)

Hubbard claims in his book that using a framework such as COSO, COCO etc. helps identify and categorize risks and controls. The organizations that are not using control frameworks rely on the skills and experience of the facilitator and work team to know when ail controls and risks have been covered. (Hubbard, 2005)

Conclusion

Considering the importance of establishing a reliable internal control system for minimization of risk and maximization of benefits; a holistic answer and a method is needed. Method should be sufficient to answer “how” questions in design of IS internal control system.

Although there are lots of information about risks, control objectives, controls and related guides; there still is a necessity for a holistic approach defining and explaining internal control system design process. An approach which brings all useful information from all these references with a method for design process will be a key for an effective internal control system.

CHAPTER 3

CONVENIENT QUALITY FOR IT GOVERNANCE AWARE COMPANIES

Introduction

IT governance processes and quality management systems (QMS) processes can be considered together by focusing on their similar aspects, thereby increasing the quality of IT processes integrated with QMS. Businesses adapt their IT processes to widely accepted frameworks and standards, such as COBIT (COBIT 4.1 Control Objectives for Information and Related Technology, 2007) and ISO 9001:2008, to prove their reliability and competence.

COBIT is regarded as an effective framework to provide IT excellence and quality. (Robinson, 2005) Stephen Reingold proposes that refining IT processes increases the quality of IT process and product quality. Moreover, their effectiveness and efficiency are improved. (Reingold, 2005) COBIT 4.1 includes maturity models for each process (based on, but in many respects quite different from, the Capability Maturity Model Integration approach) to support assessment of its current maturity state and supporting process improvement planning toward a future maturity state. This means that COBIT is used for improving systems and software quality. (Mapping of CMMI for Development V1.2 with COBIT 4.0, 2006) In light of the academic studies and case studies about COBIT 4.1, it can be seen that COBIT provides quality for IT related processes resulting in more manageable and controllable environments. To prove quality, enterprises may choose to (or be required by a key customer to) comply with ISO 9001:2008 for specific areas of their activity. Quality management models based on ISO 9001:2008 lead to much more competitive enterprises. (Wade, 2002), (Barnes, 2000). ISO 9001:2008 implementation

creates much more efficient and effective operation; increases customer satisfaction; reduces the number of audits; enhances marketing; improves employee motivation, awareness and morale; promotes international trade; increases profit; reduces waste; and increases productivity (Rohitratana, 2000). Similar to COBIT, ISO 9001:2008 has also been studied for integration with other standards. These studies aimed to provide quality for business as a whole (V.Jovanovic & D. Shoemaker, 1997) and proposed to use ISO 9001:2008 for software quality management. (B. Tam, L.Chinho, & Chin Hisang, 2003) ISO 9001:2008 is used to provide quality in e-commerce environments. A model has been developed for the compliance of these environments with ISO 9001:2008 standard. (B. Tam, L.Chinho, & Chin Hisang, 2003). However, there is not enough emphasis on the relationship between COBIT 4.1 and ISO 9001:2008. Both of these are widely used, and they focus on refining processes and aim to improve effectiveness and efficiency. Organizations can benefit from the guidance of COBIT 4.1 for IT procedures while using ISO 9001:2008 to improve their quality. Also, organizations should not use human resources (HR) more than necessary for common tasks in the proposed approach. Some IT governance processes and QMS processes can be taken into consideration and carried out together. This may simplify organizational schema for better management. Furthermore, this approach can increase communication and improve collaboration between IT and quality management departments. Therefore, this article aims to integrate processes of COBIT 4.1 and ISO 9001:2008 so organizations can increase the effectiveness and efficiency of the QMS through COBIT 4.1 control objectives.

Methodology For The Mapping

A high-level mapping is done to compare the domain areas of COBIT 4.1 with the requirements of ISO 9001:2008 by describing the overlap. COBIT 4.1 has four domain areas—Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME) (figure 1). In the framework, there are processes and related control objectives. These control objectives are affected by COBIT resources: applications, information, infrastructure and people. COBIT's information criteria (the business objectives of processing information) are listed as effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability (COBIT 4.1 Control Objectives for Information and Related Technology, 2007)

COBIT 4.1's approach is targeted at auditing, control, management and governance. ISO 9001:2008's approach is in line with COBIT 4.1's approach with respect to its management system objective subjects. ISO 9001:2008 is also focused on improving processes to increase profit and create a more efficient and effective operation. Assessments, improvements and audits based on COBIT 4.1 and ISO 9001:2008 can be taken into consideration across the organization. These assessments can be integrated, and, in this way, IT processes' quality can be made more effective and efficient—clarifying the relationship among these two references.

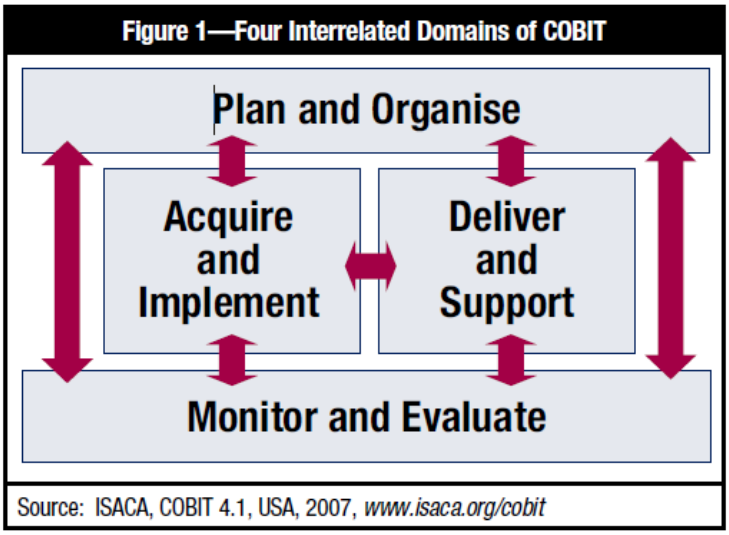

Figure 1. Four Interrelated Domains of COBIT

Figure 2—COBIT 4.1/ISO 9001:2008 Relationship

COBIT 4.1/ISO 9001:2008 Relationship	1. Quality management system	2. Management Responsibilities	3. Resource Management	4. Product Realization	5. Measurement, Analysis and Improvement
Plan and Organize	X		X		
Acquire and Implement				X	
Deliver and Support			X		
Monitor and Evaluate		X			X

Figure 2. COBIT 4.1/ISO 9001:2008 Relationship

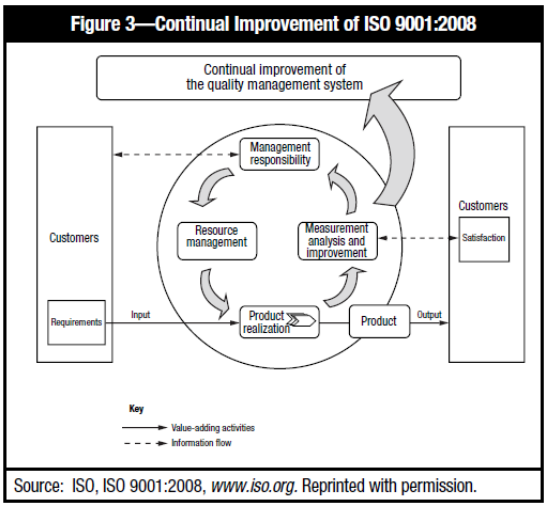

Figure 3. Continual Improvement of ISO 9001:2008

In this high-level mapping, COBIT domain areas are mapped with ISO 9001:2008 requirement areas, which are: [12]

1. Quality management system

2. Management responsibilities

3. Resource management

4. Product realization

5. Measurement, analysis and improvement

COBIT's four process domain areas have much in common with ISO 9001:2008 requirements (figure 2). COBIT 4.1 provides guidance on quality management with the help of PO8 Manage quality. In PO8, there are control system recommendations for establishment and management of a quality management system. Continual improvement of ISO 9001:2008 requirements (figure 3) are also included in PO8.5. There are several examples of the shared attributes of these two references. To illustrate, COBIT's ME domain is related to ISO 9001:2008's part 5.6 Management's Review under Management

Responsibility. In COBIT 4.1, the ME domain has control objectives for monitoring all processes to determine whether the provided direction is followed. In ISO 9001:2008's Management Responsibility part, management is also described as responsible for reviewing the system.

Both the COBIT framework and ISO 9001 stress segregation of duties to ensure clarity among roles and responsibilities. In the PO domain of COBIT, the relevant control objectives are PO4.6 establishment of roles and responsibilities and PO4.11 Segregation of duties. Similarly, in ISO 9001:2008, part 5.5 Responsibility, Authorization and Communication proposes that segregation of duties should be completed under the responsibility of management.

Service support is an important part of IT governance and, in COBIT 4.1, managing support service organizations' issues are found in the DS domain. Similarly, in part 7.4 Purchasing of ISO 9001:2008, support service organization management issues are taken into consideration. Customer satisfaction is an integral aim of ISO 9001:2008, and it is described in part 7.2 Customer Related Issues. In COBIT, customer focus is considered in PO8.4, which "focuses quality management on customers by determining their requirements and aligning them to the IT standards and practices" and defines roles and responsibilities concerning conflict resolution between the user/customer and the IT organization. [13] COBIT provides good practices across the AI domain, which "provides the solutions and passes them to be turned into services." [14] The AI domain's control objectives question if new projects deliver solutions to meet business needs and if new systems will work properly when implemented. The related portion of ISO 9001:2008 is part 7 Product Realization, which provides development stages with appropriate testing for developing new products to check whether the developed product meets the business and legal requirements and provides user satisfaction.

Part 8 of ISO 9001:2008, Measurement, Analysis and Improvement, is largely related to the ME domain of COBIT, which includes ME1 Monitor and evaluate IT performance, ME2 Monitor and evaluate internal control, ME3 Ensure compliance with external requirements and ME4 Provide IT governance. With these common requirements, both COBIT and ISO 9001:2008 focus on preventing errors by monitoring and taking remedial, corrective actions against undesirable business events.

Other than the related objectives of ISO 9001:2008 and COBIT 4.1, their affected parties and general aims show a parallelism. To illustrate, COBIT 4.1's control objectives affect application, information, infrastructure and people to provide effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability, which are also the aims of QMS.

Taking the parallel objectives of the COBIT framework and ISO 9001:2008 Quality management systems can assist with integrating these two references in assessments and reduce the time and effort spent.

Conclusion

Success in business can be achieved by improving business processes. Since IT processes are at the heart of the business life, creating more effective and efficient processes results in achievement of business objectives. By mapping the common objectives of COBIT 4.1 and ISO 9001:2008, both IT governance processes and QMS processes can be taken into consideration and carried out together, allowing one to support IT quality systems management and IT processes effectively and efficiently. Carrying the compliance efforts out in tandem can reduce the allocated time and resources for compliance studies.

CHAPTER 4

INTERNAL CONTROL DESIGN FOR INFORMATION SYSTEMS WITH CONTROL SELF-ASSESSMENT METHOD

Introduction

Being aware of the significance of IS internal control system and rapidly changing risks and opportunities IS poses to organizations; design of this system ranks higher points in importance. Organizations take control frameworks as a reference for risk management and internal control system design. Furthermore; they perceive IS control frameworks with best practices as an enabler for IS control system. Answer for "What is an effective IS internal control system?" question can be found in these reference guides. Control Practices, published by Information Systems Audit and Control Association (ISACA) [1], is an example of best control practices for Control Objectives for Information and Related Technology (COBIT) IS processes. Moreover; numerous studies can be found about evaluation of internal controls about specific information systems domain areas especially for auditors. To illustrate, "IT Assurance Guide" is a reference guide for IS auditors including how to test IS processes with detailed testing steps (ISACA, 2007). To illustrate, Ott, MacLeod and Fan studied "Computer-assisted Audit Techniques: Value of Data Mining for Corporate Auditors" (J. Ott, A. MacLeod, & K. Mar Fan, 2008)etc. IT standards, guidelines, tools, techniques, audit plan examples, control testing guides, IS best practice guides, importance of IS internal control system issues are selected as subjects for most of the studies. For example "IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals" is a guide published by ISACA, especially focusing on how to test IS, which is again a good resource explaining the best IS

control system. ISACA Journal also includes series of articles having the subject of auditing especially. For example, Singleton studied on access controls for auditors in (Singleton, 2008). However, there is little resource about designing IS control system for control system designer which can work as risk and control specialist. To illustrate; Singleton shortly touches upon the subject of control system design (Singleton, IT and Privacy Audits, 2009) (Singleton, What Every IT Auditor Should Know About IT Audits and Data, 2009). A control development life cycle model is studied which includes stages of control design, implementation, operational effectiveness, monitoring. This study aims "to enhance auditors' ability to gain assurance about the reliability of the internal control system and the individual relevant controls" (Singleton, What Every IT Auditor Should Know About Controls: The CDLC, 2009).

By looking at the quantity of academic studies and reference guides, it can be seen that much attention has been given for the evaluation of IS control system. However, the same attention should be given to design of IS control system by stressing the importance of it, since preventing undesirable events is as important as detecting those events. An effective and continuous design process can be able to decrease the number of control failures as well as to improve the controls and business processes. It can also be able to increase risk and control awareness for business owners and organization. This study provides a good introduction for CSA with examples from literature.

A Method for Internal Control Design

This study aims to open a door for risk and control specialists by giving a holistic approach for designing IS control system. By using numerous information about characteristics of

best control practices and widely accepted standards and frameworks, a method is needed for IS control system design. In the literature some methods are proposed for control system design and evaluation; one of which is CSA. To illustrate, in COBIT ME2 which is called as Evaluate Internal Control process points out to the Control Self-Assessment method as a control objective. According to Jackson; "There can be no doubt that utilizing the business excellence self-assessment models was vital for achieving the culture of continuous improvement" (Jackson, 1999).

What is CSA?

Control self-assessment, by definition, is a methodology that can be used by managers and internal auditors to assess the adequacy of an organization's risk management and control processes (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006). "It is a way of helping organizations improve their ability to meet business objectives" (J. Sheffield & S. White, 2004).

As can be seen in the definitions, CSA especially addresses internal auditors. However; Hubbard contends in his book that CSA is a tool for the entire organization and an organization can benefit from this technique with wide spread use. According to Hubbard, "CSA is a method of assessing controls in an organization that is already moving toward empowerment. CSA is not a way for internal auditing to change the culture of an organization". He claims that culture changing process belongs not to the auditors; it belongs to the management, who has the primary responsibility of the business. "CSA will help support a movement toward employee empowerment, but it is not up to the auditors to create or start that movement." (Hubbard, 2005) Sheffield and White, in their case study of

CSA implementation, conclude that "CSA has developed to become something more than an audit technique." They claim that CSA appears to be a management control and it focuses on performance, communication and feedback which promote organizational excellence (J. Sheffield & S. White, 2004).

In CSA, personnel who are actually doing the work should be involved to evaluate whether risks and controls are well balanced in achieving business objectives. Hubbard contends in his book that; it is a difference of CSA from traditional auditing; where auditors evaluate the adequacy of controls. However, experts of the business are much more knowledgeable about the problems, hindrances, risks and solutions for their work. On the other hand; Hubbard states in his book that "Auditors only come in once every few years and stay for a short time.

They are not likely to become experts in a single work process." Therefore it is very helpful involving the real experts of the business in control assessment process. Hubbard also says that "Tapping into the knowledge and experience of those experts in the area is a better way to identify the real risks and the real effectiveness of controls" (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006). In light of this information, traditional auditing approach and CSA approach responsibilities are changed. Traditionally, risk and control evaluations are done by auditors, however, in CSA; this responsibility is given to CSA work teams. Similarly, objectives of traditional audits are determined by auditors, however, in CSA, management's objectives are followed.

CSA Benefits And Concerns

CSA serves benefits and concerns for organizations. Benefits of CSA are studied in (Jordan, 1995). In CSA: A Practical guide (Hubbard, 2005) and McKeever CCSA Study system (McKeever, 2009) benefits of CSA are explained:

- Risk and control consciousness is gained for all personnel
- Control responsibility is enhanced
- Key risks about subject matter can be explored by the help of business and risk-control professionals
- Contrary to audits, personnel became more open to concentrate on risks they own
- Communication among the organization is enhanced

According to (IIA, 1998), CSA improves the control environment of an organization by:

- Enhanced understanding and awareness of organizational objectives and control roles
- Awareness of control importance in achieving goals and objectives.
- Increased personnel motivation in designing and improving controls.

According to Hubbard, the benefits also come with some concerns to be overcome (Hubbard, 2005). In CSA: A Practical guide (Hubbard, 2005) and McKeever CCSA Study system (McKeever, 2009) some examples of some concerns of CSA are explained:

- Due to incompetent business personnel involved in CSA studies, inaccurate results are gained
- Due to incompetent CSA facilitators, sharing and improving atmosphere is not established

- Management not supporting CSA studies

It is stated in the McKeever CCSA Study System book (2009), which is a study tool for certification of CSA; there are some situations that CSA does not work. These situations are fraud situations, cultural issues, compliance audit shops, inadequate resources and weak management support (McKeever, 2009).

Having the same goal of achieving business objectives, CSA and internal control design have much in common. CSA includes communication with stakeholders; it serves for control design mentality since business owners should be actively involved in this process. All decisions should be made together; business owners should approve the new or improved control designs. If a required control is not approved by business owners, they should be the primary responsible in accepting the risk in the absence of that control. For this reason, CSA can effectively be established and continued. Control self-assessment method is selected in this study since it provides a flexible solution which is especially appropriate for designing a control system to achieve changing objectives of the companies.

Factors For An Effective CSA Implementation

In order for successful implementation of CSA, there are a number of effecting factors. These are stated in Sheffield and White's study. According to this study effecting factors are:

- supportive internal culture
- a sound corporate governance framework

- the size of the organization
- the expertise of the facilitators
- a knowledgeable management
- a supportive non-executive directorate (J. Sheffield & S. White, 2004).

CSA Implementation Process

There are different approaches for the use of CSA. Many of the approaches can be used in different circumstances. According to Certification in Control Self-Assessment book, each organization should choose the most desirable approach according to their goals and scope, resources, the knowledge and skills of the staff who will be involved in the CSA process (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006).

According to Institute of Internal Auditor's (IIA) Practice Advisory, CSA is a formal, documented process designed to allow management and work teams made up of individuals from business units, functions and collaboratively

- Identify risks and exposures
- Assess the control processes that mitigate or manage those risks
- Develop action plans to reduce risks to acceptable levels
- Determine the likelihood of achieving business objectives (IIA, 2004)

In order for a CSA to be appropriate, there should be real experts from the business, there should not be a fraud situation, there should not be a rapid corporate change (since the objectives may not be clear in these situations), management support is not in place, and culture does not support effective communication.

Forms of CSA

There are three primary forms of CSA. Organizations select to use one or more forms of CSA [9]. According to the culture of the organization, the nature of the industry (highly regulated, financial, or charitable), the attitude and support of management, cost, the comfort of the audit staff, the resources of the audit shop, The attitude of the audit committee whether they believe in the success of CSA or not.

Control self-assessment provides a realistic approach for control system on the way of achieving business objectives. It includes not just auditors and risk and control specialists; it also includes business experts. This helps organizations not deviating the way of business objectives but with awareness of risks and controls which in turn results in achievement of objectives with minimum undesirable events. As indicated in Fig.1, CSA requires the commitment of the stakeholders of the business. Business stakeholders puts their knowledge about the problems, hindrances, risks and solutions for business and related objectives; risk and control professionals come with their risk and control conscience and knowledge with their facilitation and guidance skills in the CSA process.

Business experts are following up the management directions; risk and control professionals are following up international frameworks, standards, best practices, laws and regulations. Both parties share their knowledge and brainstorm to find the best results for business. This cooperation results in prevention of undesirable events and creation of effective, efficient and compliant business processes which in turn provides organization' achievement of its objectives.

Forms of the CSA are as follows which will be detailed below:

1. Facilitated Team Workshops

2. Surveys
3. Management Produced Analysis
4. Management Produced Analysis

Facilitated Team Workshops

According to IIA; facilitated team workshops are the most effective way of control self-assessments since it enhances collaboration. The facilitated team workshop process involves the CSA facilitator instructing the managers and employees on how to evaluate internal controls and risks. The facilitator guides the work team on how to design and implement effective internal controls.

The CSA facilitator attempts to focus the group's thinking and ensure that it addresses key issues.

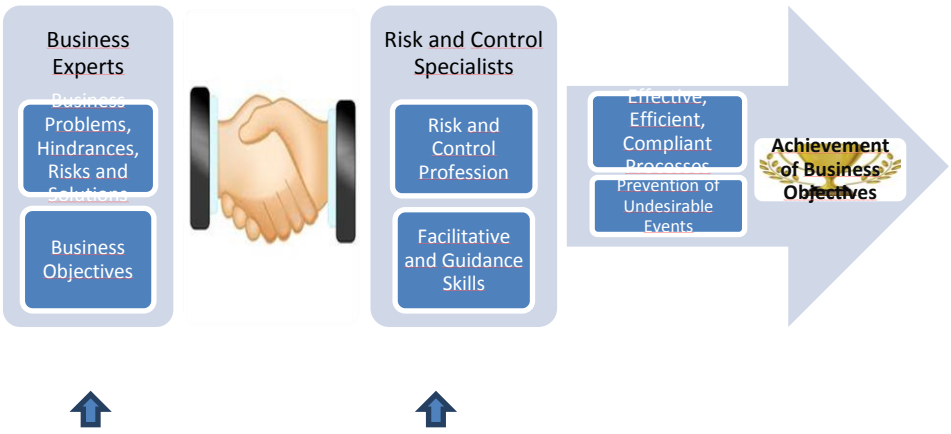

Figure 4. CSA Diagram

In Fig.1, the main objective and mentality of control self-assessment is explained. The forms of CSA will be explained below:

Objective Based

Objective based CSA workshop evaluates the control system about meeting a business objective. The present risks and the residual (remaining) risks related to the objective are identified in the first phases of the workshop. In order to meet this objective, business experts and facilitator share their knowledge to find out the possible control designs for identified risks and they try to balance the cost and benefit of the controls in order to minimize risks. The workshop aims to clarify whether the controls provide reasonable assurance. The aim of the workshop is to decide whether the types of controls currently in place are working effectively to optimize the achievement of the objective .The current residual risk may be either too high (controls are unacceptable either based on their design or their effectiveness) or too low (controls are too stringent, reducing the opportunity to achieve the objective)" (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006).

Risk Based

Risk based format of CSA takes the risks as the primary concern for the workshop. Workshop participants focus on all of the potential threats, obstacles, exposures which can be faced with in achieving a business objective. The second step is identifying the controls in place and evaluating whether the present controls are capable of minimizing those risks or they are not. "The aim of the workshop is to ensure that all significant risks are adequately managed to an acceptable level of exposure." (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006)

Control Based

Control based format takes the controls in place and their effectiveness of minimizing the related risks as focus. In this format facilitator identifies the major risks and related present controls. Workshop participants brainstorm about these controls' effectiveness and they try to determine if there are gaps in risk minimization related to the management objectives. Another topic of this workshop is determining the cost benefit analysis of the risks and controls since this also effects controls efficiency.

Process Based

Process based format takes the processes or activities as part of a process as focus of the workshop. Management's determined objectives and process control system effectiveness are evaluated in order to identify whether the controls present in the process are able to give reasonable assurance for achieving objectives. "The aim of the workshop is to evaluate, update, validate, improve, and streamline the whole process and its component activities." (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006)

Surveys

This form of CSA includes getting clear-cut answers (Yes/No, Have/Have Not etc.) from numerous business partners in order to evaluate the control system via the help of

questionnaires. This form is preferred when there are no available resources for workshops or there are "too numerous and widely dispersed" participants that hinders to bring them to a common place (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006).

According to Hubbard, "Surveys could be preferable to workshop-based CSA under some circumstances including unready organization culture for sharing of sensitive control information, unsupportive management for time allocation for CSA studies, incompetency of audit personnel for conducting CSA workshop or quick information for control system is needed (Hubbard, 2005).

Management Produced Analysis

This form of CSA "covers the approaches management uses to produce its own information and analysis about selected business processes, risk management activities and, control procedures." (J.K. Kincaid, W. J. Sampias, & A. J. Marcella Jr., 2006). Unlike workshops, management produced analysis is directed by management and prepared by an assigned team in a staff or support role. This type of format is used when there is a quick need for evaluation of internal control system related to specific area. These reports may be qualitative or quantitative. The results of these analyses can enable auditors, risk and control specialists and management to have a general understanding of internal controls in place.

Responsibilities of Workshop Facilitator

Hubbard claims that, "In general, 80 percent of what a CSA facilitator does is generic and the other 20 percent is specifically related to CSA" (Hubbard, 2005). This indicates how a

facilitator is important in accomplishing a successful workshop. Facilitator is seen as the expert for workshop facilitation, therefore s/he should have the necessary skills for managing the workshop. These skills primarily include knowledge and expertise of the workshop topic in order to accomplish the task of evaluating and designing internal control system with the workshop participants. S/he should be able to direct the meeting in order to get the most effective, efficient and compliant control system.

The facilitator's communication skill is also significant since the workshop includes several people from different business functions with different perceptions and the facilitator should manage the atmosphere with his strong communication skills. S/he is expected to encourage the group participation to get the most value from all participants. In order for all participants getting into the CSA; the facilitator should explain CSA, the aim of coming together and how they can benefit from this study. They should be convinced that it is going to be a union of forces in order to enable the achievement of business objectives. The facilitator should also resolve conflicts among participants, manage the scope, manage the time of the workshop and ensure that the subjects are handled in the meeting. The facilitator should also use his/her presentation skills to get the focus of participants to the subject, making the topic understandable and clear for all people by using presentation tools and techniques such as using slide shows, computer presentation programs etc.

Facilitator is expected to respond timely in order to take actions after the CSA workshop. S/he should prepare reports and necessary documentation and share them with the appropriate levels in the organization. Timely response is important for all participated functions to accomplish their tasks at appropriate time.

According to a research a focus group created the following profile of a CSA facilitator has skills of being smart, generalist, has ability to put structure around concepts, conversionalist, comfortable with ambiguity. This study shows that the expected personality for an effective facilitator (R. P. Tritter & D. S. Zittnan, 1996).

Facilitator, who is seen as the expert of the workshop facilitation, should be well prepared for the facilitation and has to accomplish some responsibilities. These responsibilities are meeting the logistics (including setup of the environment, organization and resource supply for meeting), explaining CSA (including explaining the aim, scope, benefits of the study and answering the questions of participants), process intervention (including personality management, solution and prevention of conflicts, rule setup and manage the time, scope of the meeting), meeting crowd control (including handling of different personalities, expectations and conflicts that can arise in meetings) (Hubbard, 2005).

Certification Opportunities For Control Specialists

In practice, much more attention is given to auditing than design in IS. Although the control system evaluation certifications for auditors such as certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA) exists for long time, the certification opportunities for risk and control specialists newly emerges. To illustrate; CISA certification, which is given by ISACA, was first established in 1978. However, certification opportunity for IS risk and control specialists was established in 2010 which is called Certified in Risk and Information Systems Control (CRISC).

Summary

This study introduces CSA with a detailed literature survey. Facilitator, who is seen as the expert of the workshop facilitation, should be well prepared for the facilitation and has to accomplish some responsibilities. These responsibilities are meeting the logistics (including setup of the environment, organization and resource supply for meeting), explaining CSA (including explaining the aim, scope, benefits of the study and answering).

Being aware of the importance of internal control system design and the need for a method which can be used by risk and control specialists; CSA is considered to be an effective approach for meeting this need. Enhancing value with union of powers from business experts and risk and control professionals by using the most appropriate form of CSA, leads to an effective, efficient and compliant control system and brings the organization to the achievement of their goals.

CHAPTER 5

PRACTICAL APPLICATION OF CSA

Introduction

According to Wallace, "operating efficiency is a primary goal of every organization. When control systems are designed, they should dovetail, as far as possible, with operations, in order to facilitate operating efficiency". (Wallace, 2005)

It is important to keep in mind that no matter how well designed and operated internal control system, cannot guarantee that an entity's objectives will be met. "This is because of inherent limitations in all internal control systems." (COSO ERM, 2004)

In order to achieve internal control system's goal of providing reasonable assurance, CSA method is recommended in this study. To provide a practical method for risk and control professionals in helping them to assess the effectiveness, efficiency of internal control system and to provide an appropriate platform for designing internal control system; application of control self-assessment method is discussed.

While performing internal control systems assessment and improvement studies; risk and control specialists should take a risk based approach. If the potential risks related with a process are more than those of the other processes and the impact of the risks are less tolerable than the others'; high risky processes should be taken into consideration as soon as possible. For this reason; risk and control specialists should make a prioritization of processes related with risk assessment just as auditors do in audits. Control self-assessment plan should be prepared and it should be in line with this process risk prioritization. According to COSO ERM framework; the majority techniques are

developed for identifying risks are performed by internal and external auditors to determine the scope of their activities using qualitative or quantitative methods to prioritize and identify higher-risk activities. However, "What is important is that management considers carefully the factors that may contribute to or increase risk." (COSO ERM, 2004). Therefore; this risk prioritization should be in line with organization's strategies and objectives. A way of achieving this is performing this risk prioritization with top management. This may not be possible; however, if the culture and management's attitude is positive, using this method will result in process prioritization which is more reflecting strategies.

In this study; the processes are not prioritized since risks change organization to organization; a prioritization should be made according to the risk level, risk appetite and control system performance of the organization. Legal and regulatory requirements should also be taken into consideration.

In planning and performing CSA studies; a project management approach can be very helpful in managing time, budget, scope and resources. Project management practices are recommended to be used in these studies. (McKeever, 2009). Scope management should be the primary concern for CSA studies since it is hard to stick to a subject in workshops where participants are coming from different departments, beliefs and knowledge areas. It is more likely to experience scope creeps in these studies. Involvement of participants selected from different departments of the organization also stresses the significance of time and resource management.

Different forms of CSA can be used in studies according to the characteristics of related process or according to the structure of the organization.

Best practices can be taken into consideration for these processes as control objectives in performing CSA studies. These best practices can give us a vision in CSA and helps us not just rely on professional expertise but also take the advantage of standards and best practices in our CSA efforts. This also helps company catch up with the continuously developing and changing IS world.

It is significant to keep in mind that communication is the critical success factor for CSA. Even if all the rules are met in the CSA process, when communication is not well managed, best performance can never be achieved from these studies. To illustrate; in some CSA workshops, participants may not be candid enough to get to the root cause. "The more candid the participants are about their processes, identifying both positives and negatives, the more likely weaknesses will be addressed." (McKeever, 2009). Collaboration with business partners and integration of professional expertise and efforts are keys to get the best performance of CSA.

Selection of CSA Type

Defined criteria should be used to select the most appropriate method of the CSA study in order to get the best results. These criteria should also be specified according to the organization's management style and its attitude towards CSA efforts.

Organization's openness is a critical concern in selecting CSA format. If the related business management is not very open for evaluating and sharing the risks and controls then the CSA workshop study may not be appropriate and results of the workshop may not be satisfying. According to IIA, CSA participants' response and acceptance are largely a

function of organizational culture as reflected in management's attitude toward the guiding principles of CSA. (IIA, 1998)

In the situations where business owners are not reluctant to share risks and existing controls via CSA studies, communication efforts should be brought forward to prepare business owners establish appropriate environment for CSA studies and convince them that these studies are not aimed just at revealing negative parts of their business, conversely; eliminating them and improving the business processes to achieve goals.

Although workshop method serves a rich environment including participants with different knowledge areas, chance to brainstorm and analyzing all aspects of the related issue; a workshop is not the right tool for every situation. (McKeever, 2009). According to the business objective, risk and control specialist should be deciding on whether workshop is appropriate or not.

To illustrate; since workshops are more costly than the other CSA forms; CSA may not be preferred in situations where risk level is extremely low to consider cost benefit balance. Workshops may not also be selected where the risk consciousness of the related process owner is very high and there may not be a need to define appropriate risk minimizing actions by such costly workshops. In these cases communication channels may be used to determine appropriate control design actions.

According to McKeever, in some situations; combination of workshops and questionnaires is the most effective tool. He also contends that there is no right or wrong combination. The most important thing in selecting the most appropriate CSA form is focusing on the objective then determining what "combination of tools is appropriate to accomplish the objective." (McKeever, 2009).

Table 1: Recommended CSA Forms Related With Appropriate Conditions

Recommended CSA Form	Appropriate Conditions
Facilitated Team Workshop	• Management style is open to share risk information • Process is owned by several departments(not too numerous) • Risk level is high • Process is complicated • Resources are available to conduct CSA
Survey	• Management style is not very open for sharing risk information • Risk level is low • Basic information of control system is needed • Quick information of control system is needed • Not available workshop resources • Too numerous process participants
Management Produced Analysis	• Quick need for evaluation of internal control system • Managements needs an analysis of business processes, risk management activities and, control procedures

Ground Rules

CSA is not an appropriate tool for some situations and does not work. Before planning a CSA; a facilitator should ensure that (McKeever, 2009);

- there is no fraud situation
- there is no rapid change situations
- there is no cultural issues
- inadequate resources
- weak management support

Ground Rules for Facilitated Teams Workshops

- Clearly inform the business stakeholders about the aim of CSA studies
- Select the most appropriate format of CSA workshop for the study (control/risk/objective/process based)
- Select the most appropriate environment for CSA workshop studies
- Invite the most appropriate personnel to CSA study who can be more valuable according to his/her business knowledge
- Be aware that a control never exists without a risk.
- Be aware that no control should be established without minimizing a risk.
- Provide examples of true life risk – impact events
- Confirm that the risk (preventing a business objective to be achieved) really exists.
- Ensure that corrective actions and control designs are confirmed by relevant stakeholders
- Ensure that corrective actions and control design responsibilities are undertaken by relevant process owners.

Ground Rules for Surveys

- Prepare clear, understandable questions
- Use language of the target audience
- Provide short and simple questions
- Prepare questions to adequately address related objectives, risks and controls.

Ground Rules For Management Produced Analysis

- Get the most up to date information in preparing analysis
- Select the most appropriate type for internal controls such as questionnaires, discussions, investigations, reviews
- Provide clear, understandable information for management to support an opinion about internal controls required by laws and regulations, external accountants etc. (Hubbard, 2005).

Facilitated Team Workshops Process

In order to provide a standard, repeatable process for control self-assessment facilitated team workshop studies and increase awareness of participants; it is important to establish a process for CSA.

It is also significant that this process should be approved by top management to make this process applicable for all departments and levels of the organization.

For this reason, following is an example of CSA workshop process. Process should be related with Risk Prioritization Process since studies should be performed according to risk level of the CSA subjects. During the facilitated team workshop process facilitator should be careful about the following points:

A Facilitator Should	A Facilitator Should Not
• help the workshop achieve its objectives • coordinate logistics • explain the CSA process • explain CSA's risk/frameworks etc. • expain voting methods • handle workshop dynamics • listen; make sure that everyone is heard • keep discussions on track • encourage all members to participate • determine strategy to get to business issues • identify critical success factors • identify barriers and work to resolve issues • encourage and foster development of other relevant ideas • understand what will work in the environment [Mckeever CSA Study System]	• answer their questions • complete someone else's sentence • influence participant' input • demonstrate lack of knowledge or belief that they know evrything about about the topic • appear withdrawn or indifferent • mishandle a participant by being short or ignoring someone who wants to speak • contradict or criticize a team member in front of team

Figure 5. A Facilitator should do and should not do

Risk Assessment

It is stated in COSO ERM framework that

“All organizations, regardless of size, structure, nature or industry, encounter risks at all levels within their organizations. Risks affect each entity’s ability to survive; successfully compete within its industry; maintain its financial strength and positive public image; and maintain the overall quality of its products, services and people.” (COSO ERM, 2004)

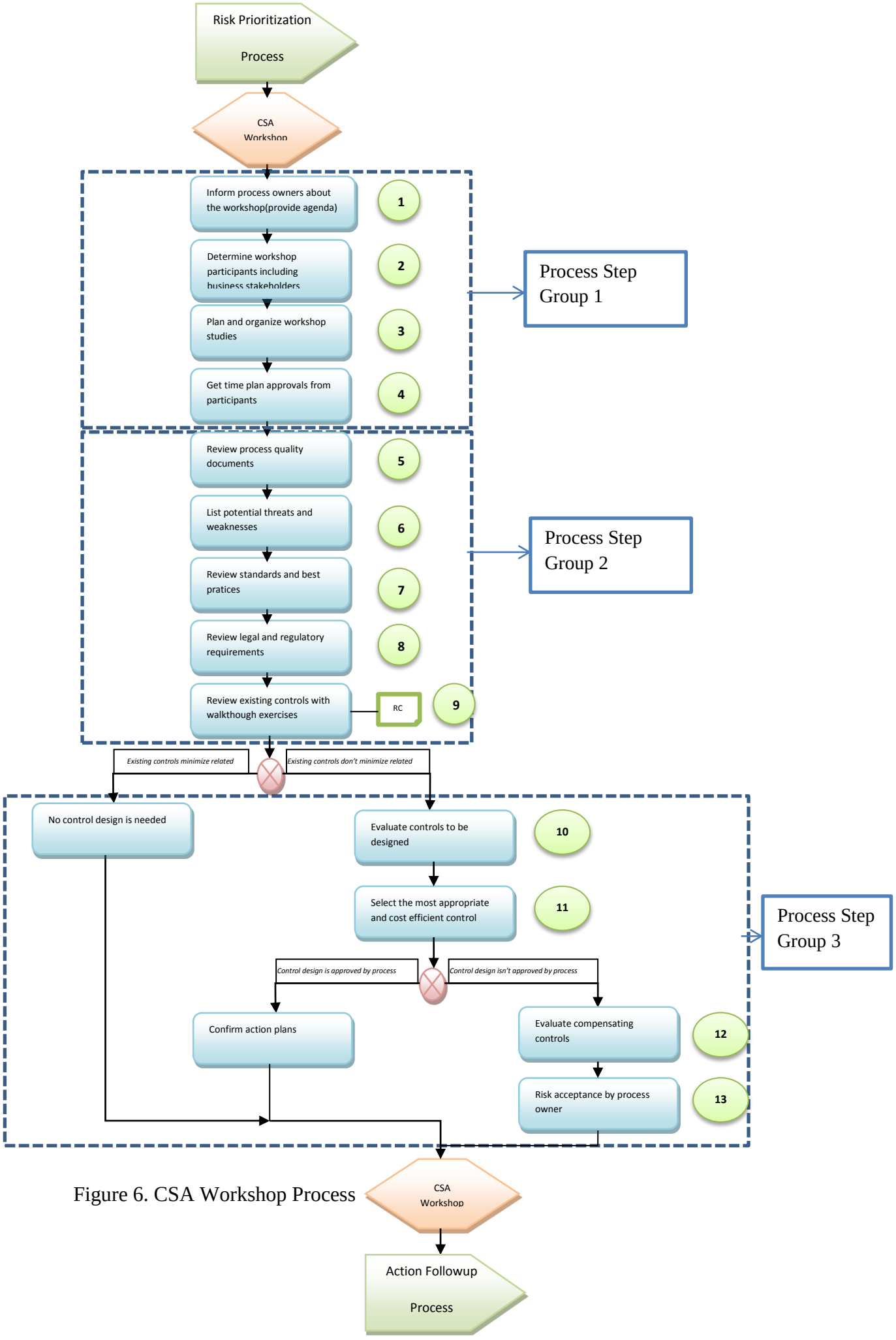

Figure 6. CSA Workshop Process

Management is responsible for identifying and performing actions needed to address the risks they assess. “The actions identified as addressing a risk also serve to focus attention on control activities to be put in place to help ensure that the actions are carried out properly and in a timely manner.” (COSO ERM, 2004)

Planning and setting environments for CSA efforts are very critical to establish a sharing atmosphere for studies. Communication and participant’s preparedness and comfort are very critical parts of the process. Therefore these steps are included in the process.

Risk management is crucial part of CSA efforts. Since controls should be designed if there is a related risk; risk assessment should be integrated to CSA studies.

Business process owners should evaluate the risks and design controls for minimizing these risks in order to achieve business objectives. In CSA studies business process owners and risk and control specialists come together to achieve this.

Risk and control specialists should be knowledgeable about types of risks since impacts of the risk types differ from organization to organization.

To illustrate; prestige risks and legal risks are not tolerable for most of the organizations which are perceived as brands.

By considering risks in CSA studies, relevance of business objectives with defined risks should be established. Risk and control specialists and participants should be sure that no risk is taken as a subject of CSA without an organizational objective. Otherwise, this means loss of efforts.

Organizations should establish their risk frameworks and risk management processes. They can select their approaches for risk management approaches such as

COSO ERM, Risk IT, ISO 31000 etc. In CSA studies, these risk evaluations should be performed in line with organization's risk management approach.

In risk assessment phase of CSA studies, organization's risk registry may be used as a tool as well as other risk declaration sources.

Some of the process steps priority order may be changed according to the workshop participants' preferences. Therefore these steps are grouped by Process Step Group 1, Process Step Group 2 and Process Step Group 3. Steps that are grouped are given below

Process Step Group 1:

- 1 Inform process owners about the workshop
- 2 Determine workshop participants including business stakeholders
- 3 Plan and organize workshop studies
- 4 Get time plan approvals from participants

Process Step Group 2:

- 5 Review process quality documents
- 6 List potential threats and weaknesses
- 7 Review standards and best pratices
- 8 Review legal and regulatory requirements
- 9 Review existing controls with walkthough exercises

Process Step Group 3:

- 10 Evaluate controls to be designed
- 11 Select the most appropriate and cost efficient control design
- 12 Evaluate compensating controls

- 13 Risk acceptance by process owner

Control Design

In relation with assessed risks, existing controls are evaluated by taking their performance of minimizing related risks. Risk and control matrixes (RCM) which provides all controls of processes can be used as a facilitating tool for CSA participants. It is important that these matrixes should be up to date.

Information sources including internal and external audit results, previous CSA results, control test results, consultancy results (if applicable), and any information provided by relevant parties (business process owners, personnel, management, customer etc.) should be taken into consideration while evaluating control's performance.

Evaluation of internal control system brings about the control deficiencies or missing controls. In case of controls not minimizing the related risks; evaluations are done for new control designs.

Wallace in her book; Internal Controls Guide; provides a broad definition of internal control definition:

> Internal controls comprise (1) the plan of organization, (2) methods and procedures adopted within a process to ensure that goals and objectives are met, (3) encouragement of adherence to prescribed managerial policies, (4) means of ensuring that there is compliance with laws and regulations, (5) methods and measures to safeguard assets against waste, loss, and misuse, (6) methods of promoting operational efficiency, (7) means of gaining assurance that data obtained, maintained, and utilized by management are complete, accurate, and reliable, and (8) means of gaining assurance that the adequacy of such data is also adequate in facilitating both the preparation of financial statements and the maintenance of accountability for assets and responsibility for liabilities. (Wallace, 2005)

Furthermore; in the book Our Perspectives on Internal Control (1989) (Wanda A. Wallace, Howard L. Siers, & William D. Hall, 1989) book, an exhibit is also provided to clarify the relationship of internal controls to control methods:

Table 2: Source: Wanda A. Wallace, Howard L. Siers, William D. Hall, James K. Loebbecke, and Keagle W. Davis, "Our Perspectives on Internal Control" (1989)

Control Methods	Broad Objectives for Control							
	1	2	3	4	5	6	7	8
Planning Systems		X						
Monitoring Systems	X	X	X	X	X	X		
Organization Structure	X	X	X		X	X		
Management Policies	X	X	X	X	X	X	X	
Management Style	X		X					
Audit Committee			X	X	X			X
Outside Advisors	X	X	X	X		X	X	
Communication Systems	X	X	X	X		X	X	
Code of Conduct	X		X	X	X	X		X
Management Information Accounting Systems (IT)		X	X	X	X	X	X	X
Budgeting Systems			X			X	X	X
Internal Audit	X		X	X	X	X	X	X
System-Level Prevention and Detection Controls			X	X	X	X	X	X
Adequate & Competent Personnel	X	X	X	X	X	X	X	X
*Key								
Create and Maintain appropriate organization and culture	1							
Set and meet corporate objectives		2						
Adherence to management's			3					

policies								
Obey laws and regulations				4				
Safeguarding of assets					5			
Operational efficiency						6		
Complete and accurate management reports							7	
Complete and accurate financial statements								8

In designing controls, all aspects of the control objectives and related control methods should be taken into consideration. This relationship [Table 3] can be used as a reference in control self-assessment workshops to evaluate existing controls and check missing controls.

Risk and control professionals should be knowledgeable about control types since type of a control is strictly related to control's operating efficiency. Types of controls with their descriptions from COSO ERM framework (COSO ERM, 2004):

Table 3: Control Types & Descriptions

Control Type	Description
Detective Control	A control designed to discover an unintended event or result (contrast with Preventive Control)
Preventive Control	A control designed to avoid an unintended event or result (contrast with Detective Control).
Computer Controls	(1) Controls performed by computer, i.e., controls programmed into computer software (contrast with Manual Controls). (2) Controls over computer processing of information, consisting of general controls and application controls (both programmed and manual).

Manual Controls	Controls performed manually, not by computer (contrast with Computer Controls (1)).

Concentrating more on preventive controls is recommended since it is better to prevent undesirable events before happening. “This proactive approach is more effective than waiting for problems to occur and then reacting to the problem after the fact.” (McKeever, 2009)

Another control type which should also be evaluated in CSA studies is compensating controls that are “intended to compensate for a weak in one control by adding another control that corrects the particular weakness” (Wallace, 2005)

Soft controls are also another type of controls which COSO addresses which are less formal and intangible. They include competence, trust and management style (McKeever, 2009). Since these are also significant for effectiveness and efficiency of internal control system, in CSA, these controls should be addressed.

Cost and Benefit Considerations For Control Design

While designing controls risk and control specialists CSA participants should take cost and benefit of intended control designs into consideration. Since internal control system is an assurance for gaining value to organizations; benefit of a control should be higher than that of the cost.

Cost of Control < Benefit of Control

This rule is also related to determining the frequency of control activities. According to Wallace, "while certain controls should be operative at all times, operating efficiency and practicality suggest that the cost of applying all controls in such a manner frequently exceeds any related benefits." This means our rule for control design is not satisfied. Wallace also contends that if personnel perceive that the controls are excessive; these controls are likely to deteriorate. For this reason, CSA participants should consider the characteristics, related risks and frequency of the business operations and then decide on the frequency of control ensuring that the benefit gained is higher than the cost of the control with its frequency.

In ensuring that benefit is higher than the cost; not only the direct cost of actually performing the control but also the indirect cost of lowering employee's morale and harming operating efficiency is evaluated. (Wallace, 2005)

In some situations appropriate control design actions may not be accepted by business process owners due to some reasons such as time, personnel, resource, and system shortages. In these cases compensating controls should be evaluated.

In these studies, monitoring controls should also be addressed. Management should be monitoring some controls to ensure that they are working as intended. This monitoring may also be addressed in case of control not sufficiently minimize related risks and when there is accepted risks.

Using Control Frameworks and Best Practices

COBIT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), COSO ERM (Committee of Sponsoring Organizations Enterprise Risk Management) IT frameworks recommend some control practices about the related process.

To take the advantage of the changing IT world and improving your processes it is recommended to review the list of best practices' control recommendations and try to design the recommended controls.

According to Hubbard there are several benefits of using a framework:

" - The control framework can act as a completeness control to be sure that all points are covered

- A framework can also be used as and aggregation tool to allow results to be accumulated over a series of different workshops using the same terminology.

- A framework can be used to form questions. This provides a structure and common terminology to workshops." (Hubbard, 2005)

Lists of best practices and standard information may be prepared as a tool to follow in workshops in order not to miss any of them and to provide a reference for all participants. This list also serves for increasing awareness of participants about international standards and extending their vision about their processes.

Documentation

Documentation is a crucial part of CSA. All precious control design and evaluation information from many expert participants may go for nothing if these are not documented in an organized manner. This documentation should include the responsibilities, risk assessments, control design decisions, risk acceptance decisions.

This documentation became an internal control system improvement tool for organizations.

Documentation style and tools differs from organization to organization. However, following should be included in CSA documentation:

- Evaluation Topic
- Related Risk and Risk Type
- Risk Evaluation
- Existing Controls Evaluation
- Risk Acceptance Decisions
- Control Design Proposals and Accepted Control Design
- Design Action Responsibilities
- Design Action Due Date
- Participant Information and Signatures

Action Followup

Action follow up is an important activity to assess the impact of CSA efforts on the company. It enables to clarify that which actions confirmed in CSA are taken. This also

brings another requirement of assessing the new established controls to realize whether they are working as confirmed and minimizing the related risk.

Ford and Evans conducted a study about the key factors of follow-up and their relationship to self-assessment outcomes which includes collecting data from 14 organizations involved in self-assessment. In order to reveal key factors of follow up activities and their relationship with CSA outcomes; follow up patterns in high and low achievers are analyzed by using qualitative data analysis methods. Study findings show that, high achievers engage in a consistent set of follow-up activities. "These activities included top management team dialogue that set the tone for follow-up, a planning process that generated a large, documented action plan, and incentive and monitoring-based implementation controls using existing structure." (M. W. Ford & J. R. Evans, 2006)

Focus Group Study

To provide a practical method for risk and control professionals in helping them to assess the effectiveness, efficiency of internal control system and to provide an appropriate platform for designing internal control system; application of control self-assessment method is evaluated in this article. In order to evaluate the effectiveness and efficiency of a sample process for practical application of Control Self-Assessment method, a focus group study is conducted.

Focus group study is selected as an academic method to get professionals' opinion about the most effective Control Self-Assessment process.

Participants are selected to be similar types of people in information systems risk, control and audit profession. Their consent is taken to participate in the focus group study.

Results are evaluated and a conclusion is drawn to clarify the necessary process steps and process step groups for effective implementation of Control Self-Assessment.

With the goal of providing an effective and efficient process for Control Self-Assessment workshop studies, a focus group study is conducted. The focus group study obtained ideas from information systems risk, control specialists auditors and consultants to test the effectiveness of proposed CSA workshop process.

Study Purpose

Purpose of this study is to evaluate the necessity, effectiveness and efficiency of the proposed Control Self-Assessment process. Process steps and process step groups are evaluated in relation with their necessity and priority. By this way a practical process for conducting Control Self-Assessment workshop studies.

Participant Characteristics

Participants of focus group study are selected according to their experience in information systems risk, control, audit, and consultancy profession (at least 3 years) and at least one certification in this field of profession.

Nine professionals attended the focus group study with an experience of 3 to 23 years with an average of 11,88 years; coming mostly from banking IS Audit, information

systems and consultancy sectors. All of the nine participants have at least one certification in risk, control, security, audit and governance areas.

Table 4: Participant Information

Participant No	Work Sector
1	IS Control
2	IS Audit
3	IS Consultancy
4	IS Control
5	IS
6	Is Control
7	IS Audit
8	IS Audit
9	IS Audit

Certifications and number of participants holding related certifications are provided below.

Table 5: Focus Group Study Participant Certification Information

Certification	Number of Participants' Certificates
CISA	6
CRISC	3
CISM	2
CGEIT	1
CISSP	2
ISO 27001	5
CRMA	1
CCSA	1
TOTAL	19

Focus Group Study Process

Before starting focus group study information about the study is provided to participants. Ground rules for the study are provided. Consent forms are signed to obtain evidence for voluntary participation. An open environment for effective participation is tried to be established. Participant privacy is stressed and information is provided that audio records will not be shared without permission. Participants are assured of complete confidentiality. (Krueger, 2002). As Krueger recommend; the focus group study pattern is selected to be (1) Welcome, (2) Overview of the topic (3) Ground rules and (4) First question.

During the focus group study an open environment for active participation is established. Contact information is provided to audience with tendering thanks to participants.

Sample Questions From The Moderator's Guide

Participants are asked to provide verbal information about the critical points of Control Self-Assessment studies including before process, during process and after process steps.

Verbal questions are provided below:

1- Is Control Self-Assessment Method is an effective method in designing and evaluating internal control system?
2- What are the most important activities to be done before Control Self-Assessment workshop to be considered as effective?

3- What are the most important activities to be done during Control Self-Assessment workshop to be considered as effective?

4- What are the most important activities to be done after Control Self-Assessment workshop to be considered as effective?

Participants are also given a list of process steps and required to check the necessity of the steps and order them to provide an effective CSA process.

Major Findings

Each of the workshop participants believes that CSA is an effective method for designing and evaluating information systems internal control system. One of the participants having 10 years-experience of IS consultancy said that Control Self-Assessment is an effective method, however, effective implementation is not a frequent condition.

Answers for the question of the most important activity for an effective CSA before the CSA process are provided below:

- Preparation for CSA process
- Preparation for laws and regulations
- Realizing about control environment
- Establishment of the CSA plan
- Determination of objectives and metrics

Answers for the question of the most important activity for an effective CSA during the CSA process are provided below:

- being sure that everybody is talking in the same language,

- making walkthroughs,
- managing time effectively
- managing different types of people
- guiding participants to the same objective

Answers for the question of the most important activity for an effective CSA after the CSA process are provided below:

- Having good relationship with decision makers
- Prioritizing action items
- Measuring the benefits after designing the controls
- Sharing of the CSA results in a timely manner
- Making action follow up
- Measuring KPIs and measuring strategic impact of designed controls
- Sharing benefits CSA results with business owners for motivation

In the focus group study participants are asked to evaluate the necessity of the process steps. Participants who agree on the necessity of the proposed process step is indicated with (+) sign and other are indicated with (-) sign. The results are provided below:

Table 6: Participant Answers to Process Step Necessity

Process Step Number	PROCESS STEPS	PARTICIPANT ANSWERS								
		1st	2nd	3rd	4th	5th	6th	7th	8th	9th
1	Inform process owners about the workshop	+	+	+	+	+	+	+	+	+
2	Determine workshop participants including business stakeholders	+	+	+	+	+	+	+	+	+
3	Plan and organize workshop studies	+	+	+	+	+	+	+	+	+
4	Get time plan approvals from participants	+	+	+	+	+	+	+	+	+
5	Review process quality documents	+	+	+	+	+	+	+	+	+
6	List potential threats and weaknesses	+	+	+	+	+	+	+	+	+
7	Review standards and best practices	+	+	+	+	+	+	+	+	+

8	Review legal and regulatory requirements	+	+	+	+	+	+	+	+	+
9	Review existing controls with walkthrough exercises	+	+	+	+	+	+	+	+	+
10	Evaluate controls to be designed	+	+	+	+	+	+	+	+	+
11	Select the most appropriate and cost efficient control design	+	+	-	+	+	+	+	+	+
12	Evaluate compensating controls	+	+	-	+	+	+	+	+	+
13	Risk acceptance by process owner	+	+	-	+	+	+	+	+	+

8 of the professionals agreed that all the process steps should be included in the process. One professional coming from IS Consultancy sector did not agree that the 11th, 12th and 13th steps are not necessary.

Analysis of answers for the last question of the study is given in [Table 7] providing the participant answers and participants who gave the same step order in the proposed CSA process are highlighted on the list. A list of process steps is introduced to the participants. The order among the process steps is asked to the participants.

Table 7: Participant Answers to Process Step Order

Process Group Number	Process Step Number	PROCESS STEPS	PARTICIPANT ANSWERS								
			1st	2nd	3rd	4th	5th	6th	7th	8th	9th
Process Step Group 1	1	Inform process owners about the workshop	8	1	3	3	1	3	1	2	1
	2	Determine workshop participants including business stakeholders	6	2	2	5	2	2	2	1	2
	3	Plan and organize workshop studies	5	3	1	4	3	1	4	3	3
	4	Get time plan approvals from participants	7	4	4	6	4	4	3	4	4
Process Step Group 2	5	Review process quality documents	1	5	7	7	7	5	6	9	5
	6	List potential threats and weaknesses	10	9	8	9	9	8	5	5	6
	7	Review standards and best practices	2	7	5	2	6	6	7	6	9
	8	Review legal and regulatory requirements	3	8	6	1	5	7	8	7	7
	9	Review existing controls with walkthrough exercises	4	6	9	8	8	9	9	8	8
Process Step Group 3	10	Evaluate controls to be designed	9	10	10	10	10	10	10	10	10
	11	Select the most appropriate and cost efficient control design	11	11	0	11	11	11	11	11	11
	12	Evaluate compensating controls	12	12	0	12	12	12	12	12	12
	13	Risk acceptance by process owner	13	13	0	13	13	13	13	13	13

Percentages of participants given the answers that are in compliance with the proposed process are calculated and also percentage of alternative answers is taken into consideration.

Participants who agree and who do not agree on the proposed process step order are provided below in [Table 8] with number and percentage information.

Table 8: Number Rate and Percentage of Participants Who Agree/Do Not Agree On the Proposed Process Step Order

Process Group Number	Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
		Number Rate	Percentage	Number Rate	Percentage
Process Step Group 1	1	4/9	44.44	5/9	55.56
	2	6/9	66.67	3/9	33.33
	3	4/9	44.44	5/9	55.56
	4	6/9	66.67	3/9	33.33
Process Step Group 2	5	3/9	33.33	6/9	66.67
	6	1/9	11.11	8/9	88.89
	7	2/9	22.22	7/9	77.78
	8	2/9	22.22	7/9	77.78
	9	3/9	33.33	6/9	66.67
Process Step Group 3	10	8/9	88.89	1/9	11.11
	11	8/9	88.89	1/9	11.11
	12	8/9	88.89	1/9	11.11
	13	8/9	88.89	1/9	11.11

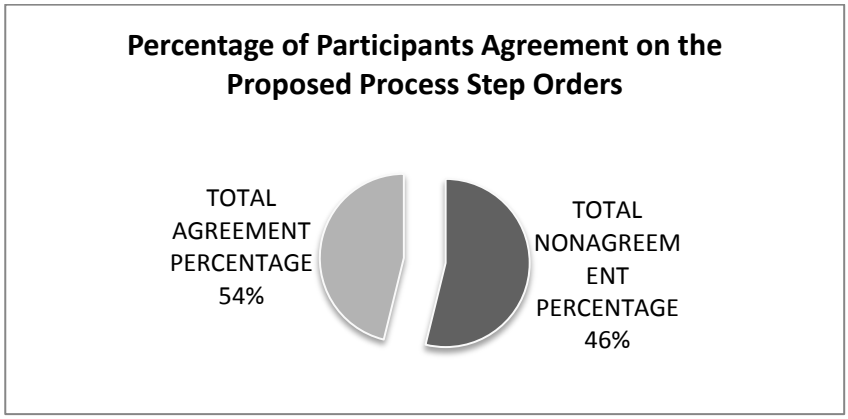

Figure 7: Percentage of Participants Agreement on the Proposed Process Step Orders

Table 9: Number Rate and Percentage of Alternative Answers Given By Participants

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS														
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	3rd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	4th Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	5th Alternative Process Step Order Proposed by Participants	Number Rate of Participants Proposed	Percentage
1	3	3/9	33.33	2	1/9	11.11	8	1/9	11.11	-	-	-	-	-	-
2	1	1/9	11.11	5	1/9	11.11	6	1/9	11.11	-	-	-	-	-	-
3	1	2/9	22.22	4	2/9	22.22	5	1/9	11.11	-	-	-	-	-	-
4	3	1/9	11.11	6	1/9	11.11	7	1/9	11.11	-	-	-	-	-	-
5	7	3/9	33.33	1	1/9	11.11	6	1/9	11.11	9	1/9	11.11	-	-	-
6	9	3/9	33.33	5	2/9	22.22	8	2/9	22.22	10	1/9	11.11	-	-	-
7	6	3/9	33.33	2	2/9	22.22	5	1/9	11.11	9	1/9	11.11	10	1/9	11.11
8	7	3/9	33.33	1	1/9	11.11	3	1/9	11.11	5	1/9		6	1/9	
9	8	4/9	44.44	4	1/9	11.11	6	1/9	11.11	-	-	-	-	-	-
10	9	1/9	11.11	-	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

- According to the results most of the participants agree 10 of the process steps (among 13) with proposed step order.
- No alternative process step is proposed by participants for 3 of the process steps.(11^{th},12^{th}, 13^{th})
- 3 of the process step orders are not agreed by most of the participants. Alternative process step order is provided by participants for 6^{th}, 7^{th} and 8^{th} process step.

Participants who agree and who do not agree on the proposed process step group order are provided below in [Table 10] with number and percentage information.

Table 10: Number and Percentage of Process Step Group Answers Given By Participants

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	8/9	88.89	1/9	11.11	83.33	16.67
	2	7/9	77.78	2/9	22.22		
	3	8/9	88.89	1/9	11.11		
	4	7/9	77.78	2/9	22.22		
Process Step Group 2	5	8/9	88.89	1/9	11.11	84.44	15.56
	6	8/9	88.89	1/9	11.11		
	7	7/9	77.78	2/9	22.22		
	8	7/9	77.78	2/9	22.22		
	9	8/9	88.89	1/9	11.11		
Process Step Group 3	10	8/9	88.89	1/9	11.11	88.89	11.11
	11	8/9	88.89	1/9	11.11		
	12	8/9	88.89	1/9	11.11		
	13	8/9	88.89	1/9	11.11		

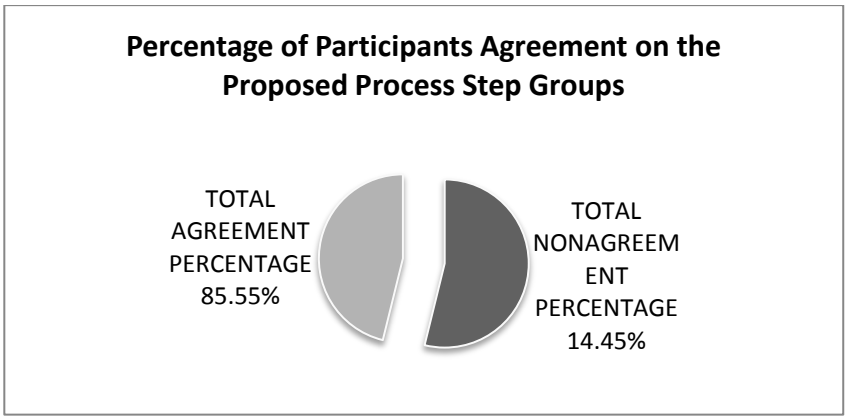

Figure 8: Percentage of Participants Agreement on the Proposed Process Step Groups

Participant answers for process groups shows that participants agree on the proposed process with a percentage of 85.55%.

Participant answers are also analyzed according to their;

- Experience(10 year experience criteria)
- Work Sector (IS Control, IS Audit, Information Systems)
- Certifications (Control , Audit, Security, IS Certifications)

Experience

Experience can be an indicator of the participants' professional expertise; therefore experience is selected as a criterion for the proposed CSA model's applicability.

Participants are divided into two categories according to their professional experience. Answers of the participant which are above 10 years and below 10 years of experience are compared.

Participant profile is provided in the below table [Table 11]

Table 11: Participant Profile for Experience Criterion

PARTICIPANT PROFILE	1st Group (Above 10 Years of Experience)	2nd Group (Below 10 Years of Experience)
Average of Experience	20.5	5
Number of Participants	4	5
Working Sectors	IS, IS Control, IS Audit, IS Consultancy	IS Control, IS Audit

Table 12: Number Rate and Percentage of Participant Answers Having More Than 10 Years of Experience for Process Steps

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	2/4	50.00	2/4	50.00
2	4/4	100.00	0/4	0.00
3	2/4	50.00	2/4	50.00
4	4/4	100.00	0/4	0.00
5	2/4	50.00	24	50.00
6	0/4	0.00	4/4	100.00
7	1/4	25.00	3/4	75.00
8	1/4	25.00	3/4	75.00
9	2/4	50.00	2/4	50.00
10	4/4	100.00	0/4	0.00
11	3/4	75.00	1/4	25.00
12	3/4	75.00	2/4	25.00
13	3/4	75.00	3/4	25.00

- According to the results; participants having more than 10 years of experience totally agree (100%) on the process step order of 1st, 4th, 10th steps.

- Most of the participants agree on the order or the process steps with are 11^{th}, 12^{th} and 13^{th} (75%).
- None of the participants agree on the order of the 6^{th} step. (0%)
- Experienced participants agree on the orders of the process steps with a percentage of 60%.

Table 13: Number Rate and Percentage of Alternative Answers for Process Step Orders Given By Participants

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS								
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	3rd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	3	2/4	50.00	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	1	2/4	50.00	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	7	2/4	50.00	-	-	-	-	-	-
6	8	2/4	50.00	9	2/4	50.00	-	-	-
7	5	1/4	25.00	6	2/4	50.00	-	-	-
8	5	1/4	25.00	6	1/4	25.00	7	1/4	25.00
9	6	1/4	25.00	8	1/4	25.00	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-

Table 14: Number Rate and Percentage of Participant Answers Having More Than 10 Years of Experience for Process Step Groups

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	4/4	100.00	0/4	0.00	100.00	0.00
	2	4/4	100.00	0/4	0.00		
	3	4/4	100.00	0/4	0.00		
	4	4/4	100.00	0/4	0.00		
Process Step Group 2	5	4/4	100.00	0/4	0.00	100.00	0.00
	6	4/4	100.00	0/4	0.00		
	7	4/4	100.00	0/4	0.00		
	8	4/4	100.00	0/4	0.00		
	9	4/4	100.00	0/4	0.00		

Process Step Group 3	10	4/4	100.00	0/4	0.00	81.25	0.00
	11	3/4	75.00	1/4	25.00		
	12	3/4	75.00	1/4	25.00		
	13	3/4	75.00	1/4	25.00		

Participant having more than 10 years of experience answers for process groups shows that participants agree on the proposed process with a percentage of 93.75%.

Table 15: Number Rate and Percentage of Participant Answers Having Less Than 10 Years of Experience for Process Steps

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	1/5	20.00	4/5	80.00
2	2/6	40.00	3/5	60.00
3	2/5	40.00	3/5	60.00
4	2/5	40.00	3/5	60.00
5	1/5	20.00	4/5	80.00
6	1/5	20.00	4/5	80.00
7	1/5	20.00	4/5	80.00
8	1/5	20.00	4/5	80.00
9	1/5	20.00	4/5	80.00
10	3/5	60.00	2/5	40.00
11	4/5	100.00	0/5	0.00
12	4/5	100.00	0/5	0.00
13	4/5	100.00	0/5	0.00

- According to the results; most of the participants agree on the order or the process steps with are 11^{th}, 12^{th} and 13^{th} (75%).

- Participants having less than 10 years agree on the orders of the process steps with a percentage of 46%.

Table 16: Number Rate and Percentage of Alternative Answers for Process Steps Given By Participants

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS											
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	2	1/5	20.00	3	1/5	20.00	8	1/5	20.00	-	-	-
2	1	1/5	20.00	5	1/5	20.00	6	1/5	20.00	-	-	-
3	4	1/5	20.00	5	1/5	20.00	-	-	-	-	-	-
4	3	1/5	20.00	6	1/5	20.00	7	1/5	20.00	-	-	-
5	1	1/5	20.00	6	1/5	20.00	7	1/5	20.00	9	1/5	20.00
6	5	2/5	40.00	9	1/5	20.00	10	1/5	20.00	-	-	-
7	2	2/5	20.00	6	1/5	20.00	9	2/5	40.00	-	-	-
8	7	2/5	40.00	1	1/5	20.00	3	1/5	20.00	-	-	-
9	8	3/5	60.00	4	1/5	20.00	-	-	-	-	-	-
10	9	1/5	20.00	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-

Table 17: Number Rate and Percentage for Process Step Groups of Participant Answers Having More Than 10 Years of Experience

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number	Percentage	Number	Percentage		
Process Step Group 1	1	4/5	80.00	1/5	20.00	70.00	30.00
	2	3/5	60.00	2/5	40.00		
	3	4/5	80.00	1/5	20.00		
	4	3/5	60.00	2/5	40.00		
Process Step Group 2	5	4/5	80.00	1/5	20.00	72.00	28.00
	6	4/5	80.00	1/5	20.00		
	7	3/5	60.00	2/5	40.00		
	8	3/5	60.00	2/5	40.00		
	9	4/5	80.00	1/5	20.00		
Process Step Group 3	10	4/5	80.00	1/5	20.00	95.00	5.00
	11	5/5	100.00	0/5	0.00		
	12	5/5	100.00	0/5	0.00		
	13	5/5	100.00	0/5	0.00		

Participant having less than 10 years of experience answers for process groups shows that participants agree on the proposed process with a percentage of 78.46%.

Comparisons of the answers are provided below [Table 18].

Table 18: Comparison of Participant Answers for Process Steps and Process Step Groups According To Experience Criterion

Process Step	Process Step Group	EXPERIENCE (Participants' % of answers agreed on proposed process step order)		EXPERIENCE (Participants' % of answers agreed on proposed process step group)	
		Above 10 Years	Below 10 Years	Above 10 Years	Below 10 Years
1	Process Step Group 1	50.00	20.00	100.00	80.00
2		100.00	40.00	100.00	60.00
3		50.00	40.00	100.00	80.00
4		100.00	40.00	100.00	60.00
5	Process Step Group 2	50.00	20.00	100.00	80.00
6		0.00	20.00	100.00	80.00
7		25.00	20.00	100.00	60.00
8		25.00	20.00	100.00	60.00
9		50.00	20.00	100.00	80.00
10	Process Step Group 2	100.00	60.00	100.00	80.00
11		75.00	100.00	75.00	100.00
12		75.00	100.00	75.00	100.00
13		75.00	100.00	75.00	100.00
TOTAL		60.00	46.00	94.23	78.46

Experienced Participants (more than 10 year) agreed more on the proposed process steps than others.

According to experience criteria; participants having experience of more than 10 years agreed on the proposed process steps with a percentage of %60 and process step groups with a percentage of 94.23 while participants having less than 10 years of

experience agreed on the proposed process steps with a percentage of %46 and process steps groups with a percentage of 78.46%.

Taking experience factor as an important indicator for processes it can be assumed that the proposed process may be applicable.

Work Sector

Work sector can be an indicator of the participants' knowledge on the subject of this study; which is Control Self-Assessment, therefore work sector is selected as a criterion for the proposed CSA model's applicability.

Participants are divided into three categories according to their professional experience. Answers of the participants which are working for the IS Audit, IS Control and IS/IS Consultancy sectors are compared.

Table 19: Participant Profile for work Sector Criterion

PARTICIPANT PROFILE	1st Group (IS Audit Professionals)	2nd Group (IS Control Professionals)	3rd Group (IS, IS Consultancy Professionals)
Average of Experience	9	8.33	23
Number of Participants	4	3	2

Table 20: Number Rate and Percentage of Participants from IS Audit Sector Who Agree/Do Not Agree On the Proposed Process Step Order

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	3/4	75.00	1/4	25.00
2	3/4	75.00	1/4	25.00
3	3/4	75.00	1/4	25.00
4	3/4	75.00	1/4	25.00
5	2/4	50.00	2/4	50.00
6	1/4	25.00	3/4	75.00
7	2/4	50.00	2/4	50.00
8	2/4	50.00	2/4	50.00
9	1/4	25.00	3/4	75.00
10	4/4	100.00	0/4	0.00
11	4/4	100.00	0/4	0.00
12	4/4	100.00	0/4	0.00
13	4/4	100.00	0.00	0.00

- According to the results; participants who work in the IS audit sector totally agree (100%) on the process step order of 10^{th}, 11^{th}, 12^{th} and 13^{th} steps.

- Most of the participants agree on the order of the process steps with are 1^{st}, 2^{nd}, 3^{rd} and 4^{th} steps (75%).

- Participants working in the IS Audit sector agree on the orders of the process steps with a percentage of 69%.

Table 21: Number Rate and Percentage of Alternative Answers Given By Participants from IS Audit Work Sector

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS (IS Auditors)					
	1st Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage
1	2	1/4	25.00	-	-	-
2	1	1/4	25.00	-	-	-
3	4	1/4	25.00	-	-	-
4	3	1/4	25.00	-	-	-
5	6	1/4	25.00	9	1/4	25.00
6	5	2/4	50.00	9	1/4	25.00
7	6	1/4	25.00	9	1/4	25.00
8	7	2/4	50.00	-	-	-
9	8	2/4	50.00	6	1/4	25.00
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-

Table 22: Number Rate and Percentage for Process Step Groups of Participant Answers from IS Audit Work Sector

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	4/4	100.00	0/9	0.00	100.00	0.00
	2	4/4	100.00	0/9	0.00		
	3	4/4	100.00	0/9	0.00		

	4	4/4	100.00	0/9	0.00		
Process Step Group 2	5	4/4	100.00	0/9	0.00	100.00	0.00
	6	4/4	100.00	0/9	0.00		
	7	4/4	100.00	0/9	0.00		
	8	4/4	100.00	0/9	0.00		
	9	4/4	100.00	0/9	0.00		
Process Step Group 3	10	4/4	100.00	0/9	0.00	100.00	0.00
	11	4/4	100.00	0/9	0.00		
	12	4/4	100.00	0/9	0.00		
	13	4/4	100.00	0/9	0.00		

Participant answers from IS Audit sector for process groups shows that participants agree on the proposed process with a percentage of 100% which means that all participants agree on the proposed model.

Results for IS Control work areas are provided below:

Table 23: Number Rate and Percentage of Participants from IS Control Sector Who Agree/Do Not Agree On the Proposed Process Step Order

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	0/3	0.00	3/3	100.00
2	1/3	33.33	2/3	66.67
3	0/3	0.00	3/3	100.00
4	1/3	33.33	2/3	66.67
5	1/3	33.33	2/3	66.67
6	0/3	0.00	3/3	100.00
7	0/3	0.00	3/3	100.00
8	0/3	0.00	3/3	100.00
9	1/3	33.33	2/3	66.67
10	2/3	66.67	1/3	33.33
11	3/3	100.00	0/3	0.00
12	3/3	100.00	0/3	0.00
13	3/3	100.00	0/3	0.00

Table 24: Number Rate and Percentage of Alternative Answers for Process Steps Given By Participants from IS Control Work Sector

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS(IS Controllers)								
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	3	2/3	66.67	8	1/3	33.33	-	-	-
2	5	1/3	33.33	6	1/3	33.33	-	-	-
3	1	1/3	33.33	4	1/3	33.33	5	1/3	33.33
4	6	1/3	33.33	7	1/3	33.33	-	-	-
5	1	1/3	33.33	7	1/3	33.33	-	-	-
6	8	1/3	33.33	9	1/3	33.33	10	1/3	33.33
7	2	2/3	66.67	6	1/3	33.33	-	-	-
8	1	1/3	33.33	3	1/3	33.33	7	1/3	33.33
9	4	1/3	33.33	8	1/3	33.33	-	-	-
10	9	1/3	33.33	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-

- According to the results; participants who work in the IS Control sector totally agree (100%) on the process step order of 11^{th}, 12^{th} and 13^{th} steps.

- Most of the participants agree on the order or the process steps with are 10^{th} step (66.67%).

- Participants working in the IS control sector agree on the orders of the process steps with a percentage of 69%.

- None of the participants agree on the step order for 1^{st}, 3^{rd}, 6^{th}, 7^{th} and 8^{th} steps. (0%).

- Most of the participants (66.67%) agree that 3^{rd} process step should be in the 1^{st} order.

- Most of the participants (66.67%) agree that 7^{th} process step should be in the 2^{nd} order.

Table 25: Number Rate and Percentage for Process Step Groups of Participant Answers from IS Control Work Sector

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	2/3	66.67	1/3	33.33	50.00	50.00
	2	1/3	33.33	2/3	66.67		
	3	2/3	66.67	1/3	33.33		
	4	1/3	33.33	2/3	66.67		
Process Step Group 2	5	2/3	66.67	1/3	33.33	53.33	46.67
	6	2/3	66.67	1/3	33.33		
	7	1/3	33.33	2/3	66.67		
	8	1/3	33.33	2/3	66.67		
	9	2/3	66.67	1/3	33.33		
Process Step Group 3	10	2/3	66.67	1/3	33.33	91.67	8.33
	11	3/3	100.00	0/3	0.00		
	12	3/3	100.00	0/3	0.00		
	13	3/3	100.00	0/3	0.00		

Participant answers from IS Control sector for process groups shows that participants agree on the proposed process with a percentage of 65%.

Results for IS / IS Consultancy sector are provided below:

Table 26: Number Rate and Percentage of Participants from IS / IS Consultancy Sector for Process Steps Who Agree/Do Not Agree On the Proposed Process Step Order

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number	Percentage	Number	Percentage
1	1/2	50.00	1/2	50.00
2	2/2	100.00	0/2	0.00
3	1/2	50.00	0/2	50.00
4	2/3	100.00	0/2	0.00
5	0/2	0.00	2/2	100.00
6	0/2	0.00	2/2	100.00
7	0/2	0.00	2/2	100.00
8	0/2	0.00	2/2	100.00
9	1/2	50.00	1/2	50.00
10	2/2	100.00	0/2	0.00
11	1/2	50.00	1/2	50.00

12	1/2	50.00	1/2	50.00
13	1/2	50.00	1/2	50.00

Table 27: Number Rate and Percentage of Alternative Answers Given By Participants for Process Steps from IS / IS Consultancy Work Sector

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS (IS Professionals/ IS Consultants)					
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	3	1/2	50.00	-	-	-
2	-	-	-	-	-	-
3	1	1/2	50.00	-	-	-
4	-	-	-	-	-	-
5	7	2/2	100.00	-	-	-
6	8	1/2	50.00	9	1/2	50.00
7	5	1/2	50.00	6	1/2	50.00
8	5	1/2	50.00	6	1/2	50.00
9	8	1/2	50.00	-	-	-
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-

- According to the results; participants who work in the IS/ IS Consultancy sector totally agree (100%) on the process step order of 2^{nd}, 4^{th} and 10^{th} steps.

- None of the participants agree on the step order for 5^{th}, 6th, 7th and 8th steps (0%).

- All the participants (100%) agree that 5^{th} process step should be in the 2^{nd} order.

Table 28: Number Rate and Percentage for Process Step Groups of Participant Answers from IS/IS Consultancy Work Sector

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number	Percentage	Number	Percentage		
Process Step Group 1	1	2/2	100.00	0/2	0.00	100.00	0.00
	2	2/2	100.00	0/2	0.00		
	3	2/2	100.00	0/2	0.00		
	4	2/2	100.00	0/2	0.00		
Process Step Group 2	5	2/2	100.00	0/2	0.00	100.00	0.00
	6	2/2	100.00	0/2	0.00		
	7	2/2	100.00	0/2	0.00		
	8	2/2	100.00	0/2	0.00		
	9	2/2	100.00	0/2	0.00		

Process Step Group 3	10	2/2	100.00	0/2	0.00	62.50	37.50
	11	1/2	50.00	1/2	50.00		
	12	1/2	50.00	1/2	50.00		
	13	1/2	50.00	1/2	50.00		

Participant answers from IS/IS Consultancy sector for process groups shows that participants agree on the proposed process with a percentage of 87.5%.

Comparison of results for the criterion of work sectors which are IS Audit, IS Control and IS/IS Consultancy. [Table 29]

Table 29: Comparison of Participant Answers According To Work Sector Criterion

Process Step	Process Step Group	WORK SECTOR (Participants' % of answers agreed on proposed process step order)			WORK SECTOR (Participants' % of answers agreed on proposed process groups)		
		IS Audit	IS Control	IS/IS Consultancy	IS Audit	IS Control	IS/IS Consultancy
1	Process Step Group 1	75.00	0.00	50.00	100.00	66.67	100.00
2		75.00	33.00	100.00	100.00	33.33	100.00
3		75.00	0.00	50.00	100.00	66.67	100.00
4		75.00	33.00	100.00	100.00	33.33	100.00
5	Process Step Group 2	50.000	33.00	0.00	100.00	66.67	100.00
6		25.00	0.00	0.00	100.00	66.67	100.00
7		50.00	0.00	0.00	100.00	33.33	100.00
8		50.00	0.00	0.00	100.00	33.33	100.00
9		25.00	33.00	50.00	100.00	66.67	100.00
10	Process Step Group 3	100.00	67.00	100.00	100.00	66.67	100.00
11		100.00	100.00	50.00	100.00	100.00	50.00
12		100.00	100.00	50.00	100.00	100.00	50.00
13		100.00	100.00	50.00	100.00	100.00	50.00
TOTAL		69	38	46	100	64.10	88.46

Participants working in IS Audit sector agreed more on the proposed process steps than others.

According to work sector criterion; participants from IS Audit sector of more agreed on the proposed process model with a percentage of %69 and process step groups with a percentage of %100 while participants from IS Control sector agreed on the model with %38 and process step groups with a percentage of 64.10% and participants from IS/

IS Consultancy sector agreed on the proposed process model with a percentage of %46 and process step groups with a percentage of 88.46%.

Certifications

Certifications can be an indicator of the participants' professional expertise; therefore certification is selected as a criterion for the proposed CSA model's applicability.

Participants are divided into four categories according to the certifications they hold. Certifications are also classified according to their related professional area; IS Audit, IS Control, IS and IS Security. Answers of the participant groups according the certifications they have are compared to assess their agreement on the proposed CSA process.

Participant profile is provided in the below table [Table 30]

Table 30: Participant Profile for Certification Criterion

PARTICIPANT PROFILE	1st Group (Having IS Audit(CISA) Certification)	2nd Group (Having IS Control Certification)	3rd Group (Having IS Certification)	3rd Group (Having IS Security Certification)
Average of Experience	17.75	12.33	17	14.71
Number of Participants	6	4	4	8
Certifications	CISA	CRISC, CCSA, CRMA, COBIT	CGEIT, ITIL	CISM, ISO 27001, CISSP

Table 31: Number Rate and Percentage of Participants from Participants Having IS Audit Certification (CISA) Who Agree/Do Not Agree On the Proposed Process Step Order

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	4/6	66.67	2/6	33.33
2	5/6	83.33	1/6	16.67
3	3/6	50.00	3/6	50.00
4	4/6	66.67	2/6	33.33
5	3/6	50.00	3/6	50.00

6	1/6	16.67	5/6	83.33
7	2/6	33.33	4/6	66.67
8	2/6	33.33	4/6	66.67
9	2/6	33.33	4/6	66.67
10	5/6	83.33	1/6	16.67
11	6/6	100.00	0/6	0.00
12	6/6	100.00	0/6	0.00
13	6/6	100.00	0/6	0.00

Table 32: Number Rate and Percentage of Alternative Answers Given By Participants for Process Step Orders from Having IS Audit Certification (CISA)

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS											
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage
1	3	1/6	16.67	9	1/6	16.67	-	-	-	-	-	-
2	6	1/6	16.67	-	-	-	-	-	-	-	-	-
3	1	1/6	16.67	4/6	1	16.67	5	1/6	16.67	-	-	-
4	3	1/6	16.67	7/6	1	16.67	-	-	-	-	-	-
5	1	1/6	16.67	6/6	1	16.67	7	1/6	16.67	-	-	-
6	9	2/6	33.33	5/6	1	16.67	8	1/6	16.67	10	1/6	16.67
7	6	2/6	33.33	2/6	1	16.67	9	1/6	16.67	-	-	-
8	7	2/6	33.33	3/6	1	16.67	5	1/6	16.67	-	-	-
9	8	2/6	33.33	4/6	1	16.67	6	1/6	16.67	-	-	-
10	9	1/6	16.67	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-

- According to the results; participants who have CISA certificate totally agree (100%) on the process step order of 11^{th}, 12^{th} and 13^{th} steps.

- Participants having IS Audit certificate (CISA) agree on the orders of the process steps with a percentage of 61.11%.

- Some of the participants (33.33%) agree that 6^{th} process step should be in the 9^{th} order.

Table 33: Number Rate and Percentage for Process Step Groups of Participant Answers Having IS Audit Certification (CISA)

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	5/6	83.33	1/6	16.67	91.67	8.33
	2	6/6	100.00	0/6	0.00		
	3	6/6	100.00	0/6	0.00		
	4	5/6	83.33	1/6	16.67		
Process Step Group 2	5	6/6	100.00	0/6	0.00	86.67	13.33
	6	5/6	83.33	1/6	16.67		
	7	5/6	83.33	1/6	16.67		
	8	5/6	83.33	1/6	16.67		
	9	5/6	83.33	1/6	16.67		
Process Step Group 3	10	5/6	83.33	1/6	16.67	95.83	4.17
	11	6/6	100.00	0/6	0.00		
	12	6/6	100.00	0/6	0.00		
	13	6/6	100.00	0/6	0.00		

Participant answers that have IS Audit certification for process step groups shows that participants agree on the proposed process with a percentage of 91.39%.

Results of certification for IS Control area is provided below:

Table 34: Number Rate and Percentage of Participants from Participants Having IS Control (CRISC, CCSA, CRMA, COBIT) Certification Who Agree/Do Not Agree On the Proposed Process Step Orders

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	2/4	50.00	2/4	50.00
2	3/4	75.00	1/4	25.00
3	2/4	50.00	2/4	50.00
4	3/4	75.00	1/4	25.00
5	1/4	25.00	3/4	75.00
6	0/4	0.00	4/4	100.00
7	1/4	25.00	3/4	75.00
8	1/4	25.00	3/4	75.00.
9	1/4	25.00	3/4	75.00
10	3/4	75.00	1/4	25.00
11	3/4	75.00	1/4	25.00
12	3/4	75.00	1/4	25.00
13	3/4	75.00	1/4	25.00

Table 35: Number Rate and Percentage of Alternative Answers Given By Participants Having IS Control Certification (CRISC, CCSA, CRMA, COBIT)

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS								
	1st Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage
1	3	1/4	25.00	8	1/4	25.00	-	-	-
2	6	1/4	25.00	-	-	-	-	-	-
3	1	1/4	25.00	5	1/4	25.00	-	-	-
4	7	1/4	25.00	-	-	-	-	-	-
5	7	2/4	50.00	1	1/4	25.00	-	-	-
6	9	2/4	50.00	8	1/4	25.00	10	1/4	25.00
7	2	1/4	25.00	5	1/4	25.00	6	1/4	25.00
8	3	1/4	25.00	5	1/4	25.00	6	1/4	25.00
9	4	1/4	25.00	6	1/4	25.00	8	1/4	25.00
10	9	1/4	25.00	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-

- According to the results; most of the participants who have CISA certificate agree (75%) on the process step order of 2^{nd}, 4^{th}, 10^{th}, 11^{th}, 12^{th} and 13^{th} steps.

- Participants having IS Control certificate (CRISC, CCSA, CRMA, COBIT) agree on the orders of the process steps with a percentage of 50%.

- None of the participants agree on the order of the 6^{th} step. Half of the participants agree that 6^{th} process step should be in the order of 9^{th}.

- Half of the participants agree that 5^{th} process step should be in the order of 7^{th}.

Table 36: Number Rate and Percentage for Process Step Groups of Participant Answers Having IS Control Certification (CCSA, CRISC, CRMA, COBIT)

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number Rate	Percentage	Number Rate	Percentage		
Process Step Group 1	1	3/4	75.00	1/4	25.00	81.25	18.75
	2	4/4	100.00	0/4	0.00		
	3	3/4	75.00	1/4	25.00		
	4	3/4	75.00	1/4	25.00		
Process Step Group 2	5	3/4	75.00	1/4	25.00	75.00	25.00
	6	3/4	75.00	1/4	25.00		
	7	3/4	75.00	1/4	25.00		
	8	3/4	75.00	1/4	25.00		
	9	3/4	75.00	1/4	25.00		
Process Step Group 3	10	3/4	75.00	1/4	25.00	93.75	6.25
	11	4/4	100.00	0/4	0.00		
	12	4/4	100.00	0/4	0.00		
	13	4/4	100.00	0/4	0.00		

Participant answers who have IS Control certification for process step groups shows that participants agree on the proposed process with a percentage of 83.33%.

Results of certification for IS area are provided below:

Table 37: Number Rate and Percentage of Participants from Participants Having IS (CGEIT, ITIL) Certification Who Agree/Do Not Agree On the Proposed Process Step Orders

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	3/4	75.00	1/4	25.00
2	4/4	100.00	0/4	0.00
3	2/4	50.00	2/4	50.00
4	3/4	75.00	1/4	25.00
5	1/4	25.00	3/4	75.00
6	0/4	0.00	4/4	100.00
7	2/4	50.00	2/4	50.00
8	2/4	50.00	2/4	50.00
9	2/4	50.00	2/4	50.00
10	4/4	100.00	1/4	25.00
11	3/4	75.00	1/4	25.00
12	3	75.00	1	25
13	3	75.00	1	25

Table 38: Number Rate and Percentage of Alternative Answers Given By Participants Having IS Certification (CGEIT, ITIL)

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS								
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	3	1/4	25.00	8	1/4	25.00	-	-	-
2	6	1/4	25.00	-	-	-	-	-	-
3	1	1/4	25.00	5	1/4	25.00	-	-	-
4	7	1/4	25.00	-	-	-	-	-	-
5	7	2/4	50.00	1	1/4	25.00	-	-	-
6	9	2/4	50.00	8	1/4	25.00	10	1/4	25.00
7	2	1/4	25.00	5	1/4	25.00	6	1/4	25.00
8	3	1/4	25.00	5	1/4	25.00	6	1/4	25.00
9	4	1/4	25.00	6	1/4	25.00	8	1/4	25.00
10	9	1/4	25.00	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-

- According to the results; all the participants who have IS certificate (CGEIT, ITIL) agree (100%) on the process step order of 2^{nd} and 10^{th} steps.

- Participants having IS certificate (CGEIT, ITIL) agree on the orders of the process steps with a percentage of 61.53%.

- None of the participants agree on the order of the 6th step. Half of the participants agree that 6th process step should be in the order of 9th.

- Half of the participants agree that 5th process step should be in the order of 7th.

Table 39: Number Rate and Percentage for Process Step Groups of Participant Answers Having IS Certification (CGEIT, ITIL)

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number	Percentage	Number	Percentage		
Process Step Group 1	1	4/4	100.00	0/4	0.00	100.00	0.00
	2	4/4	100.00	0/4	0.00		
	3	4/4	100.00	0/4	0.00		
	4	4/4	100.00	0/4	0.00		
Process Step Group 2	5	4/4	100.00	0/4	0.00	100.00	0.00
	6	4/4	100.00	0/4	0.00		
	7	4/4	100.00	0/4	0.00		
	8	4/4	100.00	0/4	0.00		
	9	4/4	100.00	0/4	0.00		
Process Step Group 3	10	4/4	100.00	0/4	0.00	81.25	18.75
	11	3/4	75.00	1/4	25.00		
	12	3/4	75.00	1/4	25.00		
	13	3/4	75.00	1/4	25.00		

Participant answers who have IS certification for process step groups shows that participants agree on the proposed process with a percentage of 93.75%.

Results of certification for IS Security area is provided below:

Table 40: Number Rate and Percentage of Participants from Participants Having IS (CISM, ISO 27001, CISSP) Certification Who Agree/Do Not Agree On the Proposed Process Step Orders

Proposed Process Step Order	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP ORDER		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP ORDER	
	Number Rate	Percentage	Number Rate	Percentage
1	3/8	37.50	5/8	62.50
2	5/8	62.50	3/8	37.50
3	3/8	37.50	5/8	62.50
4	5/8	62.50	3/8	37.50
5	2/8	25.00	6/8	75.00
6	0/8	0.00	8/8	100.00
7	2/8	25.00	6/8	75.00
8	2/8	25.00	6/8	75.00
9	3/8	37.50	5/8	62.50
10	7/8	87.50	1/8	12.50
11	7/8	87.50	1/8	12.50
12	7/8	87.50	1/8	12.50
13	7/8	87.50	1/8	12.50

Table 41: Number Rate and Percentage of Alternative Answers for Process Step Orders Given By Participants Having IS Certification (CISM, ISO 27001, CISSP)

Proposed Process Step Order	ALTERNATIVE ANSWERS GIVEN BY PARTICIPANTS														
	1st Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage	2nd Alternative Process Step Order Proposed	Number Rate of Participants Proposed	Percentage
1	3	3/8	37.50	2	1/8	12.50	8	1/8	12.50	-	-	-	-	-	-
2	1	1/8	12.50	5	1/8	12.50	6	1/8	12.50	-	-	-	-	-	-
3	1	2/8	25.00	4	2/8	25.00	5	1/8	12.50	6	1/8	12.50	-	-	-
4	3	1/8	12.50	6	1/8	12.50	7	1/8	12.50	-	-	-	-	-	-
5	7	3/8	37.50	1	1/8	12.50	6	1/8	12.50	9	1/8	12.50	-	-	-
6	9	3/8	37.50	5	2/8	25.00	8	2/8	25.00	10	1/8	12.50	-	-	-
7	6	3/8	37.50	2	2/8	25.00	5	1/8	12.50	-	-	-	-	-	-
8	7	2/8	25.00	1	1/8	12.50	3	1/8	12.50	5	1/8	12.50	6	1/8	12.50
9	8	3/8	37.50	4	1/8	12.50	6	1/8	12.50	-	-	-	-	-	-
10	9	1/8	12.50	-	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

- According to the results; most of the participants who have IS Security certificate (CISM, ISO 27001, CISSP) agree (87.5%) on the process step order of 10^{th}, 11^{th} and 12^{th} steps.

- Participants having IS Security certificate agree on the orders of the process steps with a percentage of 50.96%.

- None of the participants agree on the order of the 6^{th} step. Most of the participants agree that 6th process step should be in the order of 9^{th}.

- Half of the participants agree that 5^{th} process step should be in the order of 7^{th}.

- Half of the participants agree that 7^{th} process step should be in the order of 6^{th}.

Table 42: Number Rate and Percentage for Process Step Groups of Participant Answers Having IS Security Certification (CISM, ISO 27001, CISSP)

Proposed Process Step Group	Process Step Number	PARTICIPANTS WHO AGREE ON THE PROPOSED PROCESS STEP GROUP		PARTICIPANTS WHO DO NOT AGREE ON THE PROPOSED PROCESS STEP GROUP		Percentage of Total Process Step Group Agreement	Percentage of Total Process Step Group NonAgreement
		Number	Percentage	Number	Percentage		
Process Step Group 1	1	7/8	87.50	1/8	12.50	81.25	18.75
	2	6/8	75.00	2/8	25.00		
	3	7/8	87.50	1/8	12.50		
	4	6/8	75.00	2/8	25.00		
Process Step Group 2	5	7/8	87.50	1/8	12.50	80.00	20.00
	6	7/8	87.50	1/8	12.50		
	7	6/8	75.00	2/8	25.00		
	8	6/8	75.00	2/8	25.00		
	9	6/8	75.00	2/8	25.00		
Process Step Group 3	10	7/8	87.50	1/8	12.50	87.50	12.50
	11	7/8	87.50	1/8	12.50		
	12	7/8	87.50	1/8	12.50		
	13	7/8	87.50	1/8	12.50		

Participant answers who have IS Security certification for process step groups shows that participants agree on the proposed process with a percentage of 82.91%.

Table 43: Comparison of Participant Answers According To Certification Criterion

Process Step	Process Step Group	CERTIFICATIONS (Participants'% of answers agreed on proposed process step order)				CERTIFICATIONS (Participants'% of answers agreed on proposed process step groups)			
		IS Audit (CISA)	IS Control (CRISC, CCSA, CRMA, COBIT)	IS (CGEIT, ITIL)	IS Security (CISM, ISO 27001, CISSP)	IS Audit (CISA)	IS Control (CRISC, CCSA, CRMA, COBIT)	IS (CGEIT, ITIL)	IS Security (CISM, ISO 27001, CISSP)
1	Process Step Group 1	66.67	50.00	75.00	37.50	83.33	75.00	100.00	87.50
2		83.33	75.00	100.00	62.50	100.00	100.00	100.00	75.00
3		50.00	50.00	50.00	37.50	100.00	75.00	100.00	87.50
4		44.44	75.00	75.00	62.50	83.33	75.00	100.00	75.00
5	Process Step Group 2	50.00	25.00	25.00	25.00	100.00	75.00	100.00	87.50
6		16.67	0.00	0.00	0.00	83.33	75.00	100.00	87.50
7		33.33	25.00	50.00	25.00	83.33	75.00	100.00	75.00
8		33.33	25.00	50.00	25.00	83.33	75.00	100.00	75.00
9		33.33	25.00	50.00	37.50	83.33	75.00	100.00	75.00
10	Process Step Group 3	83.33	75.00	100.00	87.50	83.33	75.00	100.00	87.50
11		100.00	75.00	75.00	87.50	100.00	100.00	75.00	87.50
12		100.00	75.00	75.00	87.50	100.00	100.00	75.00	87.50
13		100.00	75.00	75.00	87.50	100.00	100.00	75.00	87.50
TOTAL		61.11	50	61.53	50.96	91.02	82.69	94.23	82.69

According to certification criterion; participants having IS Audit certification agreed on the proposed process step orders with a percentage of %61.11 and process step groups with a percentage of %91.02 while participants having IS Control certification agreed on the

orders with %50 and process step groups with a percentage of 82.69%. Participants having IS certification agreed on the proposed process model with a percentage of %61.53 and process step groups with a percentage of 94.23%. Participants having IS Security certification agreed on the proposed process step orders with a percentage of %50.96 and process step groups with a percentage of 82.69%.

Some additional process steps are also recommended to be involved in CSA workshop process by participants who are:

- Assessing the risk appetite (After the 10^{th} process step)
- Coordinating with risk management and organization quality process reengineering departments while communicating with business owners
- Understanding risk context (After 4^{th} process step)
- Analyzing important problems (After 5^{th} process step)

Summary

In summary, by using control self-assessment method, organization's internal control system can be evaluated and improved. Appropriate methods should be selected according to organization's management style. Objective-risk-control relationship is maintained in studies, control design actions are decided according to the related risk types and risk levels. CSA control design and improvement actions and all risk evaluations are documented as a useful internal control system evaluation tools. Action responsibilities and action dates are recorded and revised periodically.

By using this method in a standard way, it is very important to establish a standard and accepted process. Tools for evaluations, documentation, and action follow up should be developed according to organization's documentation style.

By taking the advantage of a highly qualified risk, control, audit and consultancy professionals participating in focus group study; the results can be taken into consideration to get the benefit of an effective Control Self-Assessment workshop process.

Participant answers for process groups shows that participants agree on the proposed process with a percentage of 85.55%.

Participant having more than 10 years of experience answers for process groups shows that participants agree on the proposed process with a percentage of 93.75%.

Participant having less than 10 years of experience answers for process groups shows that participants agree on the proposed process with a percentage of 78.46%.

According to experience criteria; participants having experience of more than 10 years agreed on the proposed process steps with a percentage of %60 and process step groups with a percentage of 94.23 while participants having less than 10 years of experience agreed on the proposed process steps with a percentage of %46 and process steps groups with a percentage of 78.46%.

Participant answers from IS Audit sector for process groups shows that participants agree on the proposed process with a percentage of 100% which means that all participants agree on the proposed model.

Participant answers from IS Control work sector for process groups shows that participants agree on the proposed process with a percentage of 65%.

Participant answers from IS/IS Consultancy sector for process groups shows that participants agree on the proposed process with a percentage of 87.5%.

According to work sector criterion; participants from IS Audit sector of more agreed on the proposed process model with a percentage of %69 and process step groups with a percentage of %100 while participants from IS Control sector agreed on the model with %38 and process step groups with a percentage of 64.10% and participants from IS/ IS Consultancy sector agreed on the proposed process model with a percentage of %46 and process step groups with a percentage of 88.46%.

Participant answers that have IS Audit certification for process step groups shows that participants agree on the proposed process with a percentage of 91.39%.

Participant answers who have IS Control certification for process step groups shows that participants agree on the proposed process with a percentage of 83.33%.

Participant answers who have IS certification for process step groups shows that participants agree on the proposed process with a percentage of 93.75%.

Participant answers who have IS Security certification for process step groups shows that participants agree on the proposed process with a percentage of 82.91%.

According to certification criterion; participants having IS Audit certification agreed on the proposed process step orders with a percentage of %61.11 and process step groups with a percentage of %91.02 while participants having IS Control certification agreed on the orders with %50 and process step groups with a percentage of 82.69%. Participants having IS certification agreed on the proposed process model with a percentage of %61.53 and process step groups with a percentage of 94.23%. Participants

having IS Security certification agreed on the proposed process step orders with a percentage of %50.96 and process step groups with a percentage of 82.69%.

According to the results Control Self-assessment is considered to be an effective method for IS internal control system design and evaluation. Effective management of CSA process determines the success of CSA process. Realizing and communicating the benefits of CSA studies and designed control are mostly proposed to motivate participation of CSA studies.

The proposed process model gained 53.84% agreement on the process steps and orders. Taking the experience, work sector and certification factors into consideration proposed process process step orders and necessity of the steps can be considered according to the organizations custom environment.

Organizations can add other steps to this process to customize it to their needs. Focus group study results tells us that; some proposed step orders can be swapped with the alternative process steps provided by participants and alternative Control Self-Assessment processes can be used as an IS internal control system design and evaluation tool.

CHAPTER 6

CRITICAL INFORMATION SYSTEMS PROCESSES

Introduction

Organizations maintain their operations by the help of processes according to their working styles. A process can be defined as follows: “For an organization to function effectively, it has to determine and manage numerous linked activities. An activity or set of activities using resources, and managed in order to enable the transformation of inputs into outputs, can be considered as a process.” (ISO, 2008). Processes may differ from organization to organization according to their organizational structure, business objectives and working styles. Furthermore, processes for managing information technology (IT) operations should be formed since IT is a part of every business process. Such processes will be described here, that can be considered as critical from the viewpoint of using confidential information in business operations. These processes have been defined taking into account those requirements that are acknowledged by most of the well-known information technology frameworks and standards. These methods usually differ according to their approach to problem solving and to their targeted audience, too (Erdélyi, 2010), but here the most important common issues have been taken into consideration.

According to COBIT 4.1 (COBIT 5.0 A Business Framework for the Governance and Management of Enterprise IT, 2012) critical IT processes concept is stressed and required under many control objectives. To illustrate; in PO4.11 importance of segregation of duties, in PO7.5 dependence upon individuals for critical processes, in ME2.2 managerial oversight for critical processes are stated.

In newly announced COBIT 5.0 (COBIT 5.0 A Business Framework for the Governance and Management of Enterprise IT, 2012) framework, the concept of critical IT processes is also stressed such as in DSS01.02, (integration of critical internal IT management processes with those of outsourced service providers). In MEA01; percent of critical processes monitored and in MEA02; percent of critical business processes covered by risk assessment are defined as a process performance metric.

Fundamental processes for IT operations in this study are given as follows:

1. Determining the IT Strategy
2. The Project and Program Management Process
3. The Change Management Process
4. The Third-party Service Management Process
5. The Continuous Service Assurance Process
6. The Information Security Management Process
7. The Configuration Management Process
8. The Problem Management Process
9. The Data Management Process
10. The Physical Environment Management Process
11. The IT Operations Management Process

In order to use best practices and take the advantage of improving business; frameworks and standards developed for process management, information systems management, and information technology governance. These frameworks provide a general understanding of necessary processes needed to be established in organizations. The critical processes which are addressed in this document are listed below according to their presence in the best known frameworks such as Control Objectives for Information and Related Technology (COBIT) which is a generally accepted IT governance framework? Project Management

Body of Knowledge (PMBOK) is also a widely accepted project management framework added in the list. Capability Maturity Model Integration (CMMI) is a process improvement capability maturity model and IT Infrastructure Library (ITIL) is the most widely accepted approach to IT service management in the world take place in the following list. ISO 27001 is also included in the list which is a widely accepted Information Security Management Standard. TOGAF is a detailed method and set of supporting tools for developing enterprise architecture, developed by members of The Open Group, working within the Architecture Forum (ISACA). Lastly ISO 9001:2008, the most widely accepted quality management standard is added in the list.

The selected fundamental information systems processes are mostly included in these well-known frameworks and standards. Brief description of the processes and their relation with business will be explained.

Table 44: Presence of Critical Processes in Well-Known Frameworks

IS Process Name	COBIT	PMBOK	CMMI	ITIL	ISO 270001	TOGAF	ISO 9001:2008
Determining the IT Strategy	+	+	+	+	-	+	-
The Project and Program Management	+	+	+	+	-	+	+
The Change Management	+	+	+	+	+	+	+
The Third-party Service Management	+	+	+	+	+	+	+
The Continuous Service Assurance	+	+	-	+	+	+	+
The Information Security Management	+	+	-	+	+	+	-
The Configuration Management	+	+	+	+	+	+	-
The Problem Management	+	+	+	+	+	-	-
The Data Management	+	+	-	+	+	+	+
The Physical Environment Management	+	+	-	+	+	+	-
The IT Operations Management	+	-	-	+	+	+	+

Determining IT Strategy

Strategy is the first step in determining the organization's direction and as stated in Gold's article "Technology has become so embedded in the internal functions and the external value propositions of modern organizations that it is impossible to execute strategy in any organization without it". (S.Gold, 2002). IT strategy should be in line with the

organization's objectives in order support business in achieving the strategic goals of the company. There should be a clear strategy information transfer for organization management to IT management and mechanisms to align these strategies should be in place. There should be no discrepancies between the organization and IT strategy since it will conflict with the aim of getting through the determined direction. A strategy plan should be developed and regularly updated for compliance with changing business needs and objectives.

This process should also comply with the new competitive changes in the environment and should provide for updating the strategy according to these changes to catch up with the changing world.

The Project and Program Management Process

Business objectives can only be achieved by following the business strategy. As Hardy indicates in his article; "If IT is to deliver the services that a business needs now and in the future, it has to be managed by the business as a whole." (Hardy, 2002) This can be done by allocating resources and budget in line with business priorities. Doing the right projects with the right prioritization is significant, therefore; project and program management plays crucial role. Project planning, project's relationships, resource planning, project budgeting should be done according to business priorities. Requirements planning, risk management, testing, quality management and stakeholder approval phases have critical importance on the project's success. Project's success should be reviewed in order to ensure the value is delivered to the organization.

The Change Management Process

Since business environments undergo rapid changes, organizations are expected to adapt to this changing world. To adopt these changes, organizations try to reevaluate business goals and direction. This makes change management process crucial since catching up with this rapid changing world carries new risks and opportunities to the organization which must be followed and managed effectively. According to Kulkarni; "Competitive pressures, rising expectations from global customers and the emergence of newer technologies, especially in the area of telecommunication, have accelerated the process of change management." (Kulkarni, 2003). Being aware of the speed of the IS environment, change management's importance is revealed. In order to manage changes to take the advantage for business and minimize the related risks this process should involve some phases. Monitoring and taking change requests, prioritizing them, evaluating the change impact, taking the appropriate stakeholder approvals, tracking the status of the changes in order to ensure that they are done as planned and reporting all belong to the phases of a change management process.

The Third-Party Service Management Process

As organizations focus on their primary service area they may get some outsource support for their operations. This is very common in information technology area since IT is an integral part of business operation support. Since third party services directly affect the organization's business operations, management of these services is very significant. Every detail about the service requirements, roles and responsibilities, communications, legal obligations, payment, support and cancellation should be determined and written into the contract. This process should also include compliance monitoring of the third party

contracts. According to Parks, “Properly constituted organizations have the capacity to enter into contracts with one another, and many legal endeavors go into working out the terms of the contract, as well as assessing how its terms are complied with during the duration of the contract.” (Parkes, 2004)

The Continuous Service Assurance Process

Sayana contends that “The confidentiality, integrity and availability of information systems must be ensured to protect the business from the risks relating to information technology.” (Sayana, 2005). Organizations may face some disruptions such as natural disasters, service outages. Organizations should take precautions for not reflecting these disruptions to their customers and provide service continuity. This needs to determine critical business processes and continuously backing up them in an alternative site, which is away from the risks of main site. Roles and responsibilities are very important in the event of a disruption; all critical personnel should know how to act. Manuals and communication information should be in place at their homes and at the alternative site. Continuity should be periodically tested to ensure its applicability. The business continuity plan should be clearly documented and periodically updated. This process is very significant since organizations are expected to serve the customer continuously and cope with these disruptions.

The Information Security Management Process

Information is the most important asset of the organizations; it is indispensable in their operations. There are remarkable issues to consider in using information technology as a

support for business operations. IT assets should be protected against vulnerabilities and incidents in order to minimize the business impact of damaged security. (COBIT 4.1 Control Objectives for Information and Related Technology, 2007). According to Srinivasan, information systems security management belongs essentially to risk management, handling the threat of attacks on the system, and dealing with the threat posed by vulnerabilities. (Srinivasan, 2008)

This process should include determining security roles and responsibilities, information security rules, procedures, policies and standards. Monitoring noncompliance to security policies and related rules, periodically testing for ensuring the safety of information systems should be established in the organization. Corrective and improvement actions should be followed up in order to ensure that the risks are minimized. Security management should be done effectively in order to ensure the protection of information assets and continuity of services. To accomplish this hard task in today's risky technology environment, new risks and threats should be continuously followed and appropriate mechanisms should be alerted rapidly.

The Configuration Management Process

Providing for system availability, production issue management, recovering from erroneous operations is very important for business continuity, safety and customer satisfaction. Configuration management process aims at an accurate and complete configuration inventory. Backing up the configuration information is a part of this process which helps returning back whenever a problem occurs. Integrity of these configurations should also be monitored and tested periodically as a part of this process.

The Problem Management Process

It is common to face problems in ongoing business operations related to information technology. Organizations establish problem management process to turn back to normal operation of business activities as soon as they can. Recognizing the problem, communication of the problem to appropriate parties, root cause analysis, determining the solution, taking the appropriate stakeholder approval for solution, resolving the problem, monitoring of the status, closing the problem are important stages of the process. Documentation and reporting for knowledge sharing is also significant for this process in order to accelerate the resolution of known problems.

Periodically analyzing the problems encountered can result in process improvements which can improve organization's ability to perform business activities.

The Data Management Process

An entity's information assets constitute a significant proportion of an entity's market value (ITGI, 2001) making this a key enterprise asset that needs to be governed effectively. (ITGI, 2001). Business operation's quality is strictly related to the timeliness, availability, quality of business data. Accuracy, consistency, completeness, confidentiality, integrity and availability are desired characteristics of data to be provided for business use. In order to accomplish this task it is important to establish a data management process. This process should involve determining the data storage and retention requirements with business management, establishing and maintaining a media library, protecting, backing up, restoring and disposing of data and sensitive media.

The Physical Environment Management Process

Physical facilities should be managed in order to protect and computer and related equipment. Appropriate physical conditions should be selected for business continuity. Computer and related equipment should operate effectively in the selected environment. Establishing and maintaining this process could help organizations to minimize the damages to the physical facilities and hence to minimize the interruptions to the business operations. Protection of the physical facilities includes physical facility staff protection. This process also reduces organization's resource allocation for maintenance.

The IT Operations Management Process

"Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware." (COBIT 4.1 Control Objectives for Information and Related Technology, 2007). This process is crucial since operating policies, procedures needs to be defined and done in a standard way which helps safe continuation of business activities. Scheduled processing management takes place in this process which is very critical for business operations. Performance monitoring for infrastructure and related technology should be established and information mechanism for the detected events should be set up. In COBIT 4.1 manual, it is claimed that "effective operations management helps maintain data integrity and reduces business delays and IT operating costs."

Plans For The Future

Perhaps the most important improvement will be the extension of the domain and range of these processes from the IT arena towards corporate operations.

Another - practical - direction is the extension of the set of requirements that these processes represent.

Change management can be considered to be one of the components of a more general criterium, that is also applicable to characterize excellence - both on the IT, or on the operations area - this is criterium documentation, that had been introduced in 2011 (Szenes, 2011). Besides change management, to this criterium belongs configuration management, too, among others. Following this line, these processes can be extended, on the one hand, from IT to the whole operations arena, as it had already been done with some of the basic notions of IT audit and security (Szenes, Supporting Applications Development and Operation Using IT Security and Audit Measures, 2011), and, from the other hand, the extension of the processes can be aligned to the excellence criteria, that are relevant to the given fundamental process. Investigating the positive effect of these processes, such criteria, that might characterize operational improvements, could be handy.

Classifying the scope of operations, the domain of these fundamental processes could be decomposed; these components of the domain might facilitate the application of these processes in the everyday life of a company. A possible partition can be three pillars: the organizational, the regulational, and the technical pillar. First these had been defined as pillars of IT, then they had been generalized ton pillars of operations (Szenes, IT GRC versus ? Enterprise GRC but: IT GRC is a Basis of Strategic Governance, 2010) (Szenes, Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities, 2011)

APPENDIX

A. Focus Group Study Participation Form

ODAK GRUP GÖRÜŞMESİ KATILIM KABUL FORMU

Bu çalışma Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri, Sosyal Bilimler Enstitüsü- Yönetim Bilişim Sistemleri öğrencisi olan Tuğba YILDIRIM'IN yüksek lisans tezi kapsamında gerçekleştirilmektedir. Odak grup çalışması yapılacak olan tez "Kontrol Özdeğerlendirme Metodu Kullanılarak Bilgi Sistemleri Süreçleri için İç Kontrol Sisteminin Değerlendirilmesi ve Tasarlanması" konusunu ele almaktadır.

Bu çalışma söz konusu teze ilişkin veri elde etmek üzere hazırlanmıştır ve sizlerin gönüllü olarak katılımınız beklenmektedir.

- Bu çalışmanın amacı Bilgi Sistemlerine yönelik İç Kontrol Sisteminin tasarlanmasında ve değerlendirilmesinde Kontrol Öz değerlendirme Metodunun kullanımına ilişkin etkin olabilecek bir sürecin tasarlanması için süreç içerisinde var olması gereken adımlarını belirlemektedir.
- Çalışma esnasında vereceğiniz bilgiler tamamen gizlidir ve çalışma sürecinde ileteceğiniz bilgiler sizin namınızda kesinlikle hiçbir şekilde paylaşılmayacaktır.
- Konuya ilişkin fikirlerinizin, görüşlerinizin bütün bir şekilde çalışmaya dâhil edilebilmesi için kayıt altına alınacaktır ve dokümante edildikten sonra bu kayıtlar silinecektir.
- Çalışmanın herhangi bir aşamasında cevap vermeyebilir veya katılımdan vazgeçebilirsiniz.
- Çalışma sürecinde sağlanan bilgilerin gizliliğine yönelik olarak tüm katılımcılardan bu süreçte paylaşılan bilgilerin gizli tutulmasına yönelik özeni göstermesini beklemekteyiz.
- Şimdi veya çalışma sonrasında herhangi bir sorunuz olması halinde benimle paylaşabilirsiniz veya bu formun sonunda belirtilen e-posta adresini kullanarak iletişim kurabilirsiniz.
- Lütfen çalışmaya katılmayı onayladığınıza dair onay kutusunu işaretleyiniz.

Ad :

Soyad :

Katılım Onayı : Evet □ Hayır □

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?

2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?

3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması öncesinde yapılması gereken en önemli aktiviteler nelerdir?

4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması sürecinde öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?

5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması sonrasında hangi aktivitenin gerçekleştirilmesi gerekmektedir?

6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;

- **a.** Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
- **b.** Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-…)	İşlem Adımları
		Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
		Atölye çalışması katılımcıların belirlenmesi
		Atölye çalışmalarının planlanması ve organize edilmesi
		Katılımcılardan zaman planına yönelik onay alınması
		Süreç kalite dokümanlarının incelenmesi
		Potansiyel tehditler ve açıklıkların belirlenmesi/listelenmesi
		Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
		Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
		Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
		Tasarlanması beklenen kontrollerin değerlendirilmesi
		En uygun ve maliyet-etkin kontrollerin tasarlanması
		Dengeleyici(Telafi edici kontrollerin tasarlanması)
		Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

B. Focus Group Participation List

KATILIMCI LİSTESİ

AD-SOYAD	SEKTÖR	TECRÜBE YILI	SERTİFİKA BİLGİLERİ	KATILIM
[illegible]	Bankacılık	24	-	✓
Serap Çobat	Bankacılık	3	ISO 27001	✓
Cevat Öz	Bankacılık	4	CISA	✓
[illegible]	Bankacılık	18/20	CISA, CRISC, [illegible]	✓
Aslı [illegible]	Denetim	23	CISA, CISM, CISSP, CRISC, CDEI, ISO 27001, CA	✓
Mehmet [illegible]	Bilgi Bilişim	7	ISO 27001	✓
Tansel Kılıçer	Danışmanlık	23	COBIT, ITIL, ISO 27001	✓
Uğur Kağan Dinçsoy	Denetim	7	CISA, ITIL, ISO 27001 LA	✓
Cevat İLGAZ	Bankacılık	18	CISA, CISSP	✓

C. Focus Group Study Forms

Participant 1:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması öncesinde yapılması gereken en önemli aktiviteler nelerdir? Ön hazırlık
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması sürecinde öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir? Kuralların açıklanması
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması sonrasında hangi aktivitenin gerçekleştirilmesi gerekmektedir? aksiyonların takibi
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

	a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
1	+	8	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
2	+	6	Atölye çalışması katılımcıların belirlenmesi
3	+	5	Atölye çalışmalarının planlanması ve organize edilmesi
4	+	7	Katılımcılardan zaman planına yönelik onay alınması
5	+	1	Süreç kalite dokümanlarının incelenmesi
6	+	10	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
7	+	2	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
8	+	3	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
9	+	4	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
10	+	9	Tasarlanması beklenen kontrollerin değerlendirilmesi
11	+	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
12	+	12	Dengeleyici/Telafi edici kontrollerin tasarlanması
13	+	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

Participant 2:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
✓	1	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
✓	2	Atölye çalışması katılımcıların belirlenmesi
✓	3	Atölye çalışmalarının planlanması ve organize edilmesi
✓	4	Katılımcılardan zaman planına yönelik onay alınması
✓	5	Süreç kalite dokümanlarının incelenmesi
✓	9	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi → Risk havuzu
✓	7	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
✓	8	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
✓	6	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
✓	9.5 / 10	→ Risk istahının değerlendirilmesi Tasarlanması beklenen kontrollerin değerlendirilmesi
✓	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
✓	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
✓	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbamotu@gmail.com

Participant 3:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gerekllik (+/-)	b.Sıralama (1-...)	İşlem Adımları
+	3	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	2	Atölye çalışması katılımcıların belirlenmesi
+	1	Atölye çalışmalarının planlanması ve organize edilmesi
+	4	Katılımcılardan zaman planına yönelik onay alınması
+	7	Süreç kalite dokümanlarının incelenmesi
+	8	Potansiyel tehditler ve açıklıkların belirlenmesi/listelenmesi
+	5	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	6	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	9	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
-		En uygun ve maliyet-etkin kontrollerin tasarlanması
-		Dengeleyici(Telafi edici kontrollerin tasarlanması)
-		Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

10 Kontrollerin Tasarlanması

İletişim: tugbametu@gmail.com

Participant 4:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-..)	İşlem Adımları
+	3	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	5	Atölye çalışması katılımcıların belirlenmesi
+	4	Atölye çalışmalarının planlanması ve organize edilmesi
+	6	Katılımcılardan zaman planına yönelik onay alınması
+	7	Süreç kalite dokümanlarının incelenmesi
+	9	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
+	2	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	1	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	8	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
+	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
+	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
+	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

Participant 5:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
+	1	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	2	Atölye çalışması katılımcıların belirlenmesi
+	3	Atölye çalışmalarının planlanması ve organize edilmesi
+	4	Katılımcılardan zaman planına yönelik onay alınması
+	7	Risk contextinin anlaşılması Süreç kalite dokümanlarının incelenmesi
+	9	Süreçte önceki problemlerin incelenmesi Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
+	6	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	5	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	8	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
+	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
+	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
+	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

Participant 6:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
+	3	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	2	Atölye çalışması katılımcıların belirlenmesi
+	1	Atölye çalışmaları nın planlaması ve organize edilmesi
+	4	Katılımcılardan zaman planına yönelik onay alınması
+	5	Süreç kalite dokümanlarının incelenmesi
+	8	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
+	6	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	7	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	9	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
+	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
+	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
+	13	Süreç sahibi tarafından artık riskler in kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

Participant 7:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
	1	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
	2	Atölye çalışması katılımcıların belirlenmesi
	4	Atölye çalışmalarının planlanması ve organize edilmesi
	3	Katılımcılardan zaman planına yönelik onay alınması
	6	Süreç kalite dokümanlarının incelenmesi
	5	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
	7	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
	8	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
	9	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

4* Risk yönetimi ve organizasyon süreç politika ekiplerinde

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

4= 32 değerlendirme sonucunda iş birimlerine onaylatılması koordine olarak süreçte ulaşılması (sadece yeni kontroller değil var olan tüm kontroller için sonuca

İletişim: tugbametu@gmail.com

Participant 8:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz? (1-Birinci, 2-sonraki,?)

a.Gerekilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
+	1-b	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	1-a	Atölye çalışması katılımcıların belirlenmesi
+	1-c	Atölye çalışmalarının planlanması ve organize edilmesi
+	1-d	Katılımcılardan zaman planına yönelik onay alınması
+	2-i	Süreç kalite dokümanlarının incelenmesi
+	2-e	Potansiyel tehditler ve açıklıkların belirlenmesi/listelenmesi
+	2-f	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	2-g	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	2-h	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	3-j	Tasarlanması beklenen kontrollerin değerlendirilmesi
+	3-k	En uygun ve maliyet-etkin kontrollerin tasarlanması
+	3-l	Dengeleyici(Telafi edici kontrollerin tasarlanması)
+	3-m	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

Participant 9:

SORULAR

1- Denetim ve kontrol alanında herhangi bir sertifikaya sahip misiniz?
2- Kontrol Öz değerlendirme çalışmalarının iç kontrol sisteminin tasarlanması ve değerlendirilmesinde etkin bir metot olduğunu düşünüyor musunuz?
3- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılacak bir atölye çalışması **öncesinde** yapılması gereken en önemli aktiviteler nelerdir?
4- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sürecinde** öncelikli olarak hangi aktivitenin gerçekleştirilmesi gerekmektedir?
5- Kontrol Öz değerlendirme sürecinin beklenen amacı sağlayabilmesine yönelik olarak yapılan bir atölye çalışması **sonrasında** hangi aktivitenin gerçekleştirilmesi gerekmektedir?
6- Aşağıdaki işlem adımlarından bir Kontrol Özdeğerlendirme Atölye çalışmasında;
   a. Gerekli olmadığını düşündüğünüz adımları işaretler misiniz?
   b. Olması gereken adımları önceliklendirir misiniz?

a.Gereklilik (+/-)	b.Sıralama (1-...)	İşlem Adımları
+	1	Süreç sahiplerine atölye çalışmasına ilişkin bilgilendirme yapılması
+	2	Atölye çalışması katılımcıların belirlenmesi
+	3	Atölye çalışmalarının planlanması ve organize edilmesi
+	4	Katılımcılardan zaman planına yönelik onay alınması
+	5	Süreç kalite dokümanlarının incelenmesi
+	6	Potansiyel tehditler ve açıkların belirlenmesi/listelenmesi
+	9	Konuya ilişkin standart ve en iyi uygulamaların gözden geçirilmesi
+	7	Konuya ilişkin yasa ve düzenlemelerin gözden geçirilmesi
+	8	Walkthrough çalışmalarıyla mevcut kontrollerin gözden geçirilmesi
+	10	Tasarlanması beklenen kontrollerin değerlendirilmesi
+	11	En uygun ve maliyet-etkin kontrollerin tasarlanması
+	12	Dengeleyici(Telafi edici kontrollerin tasarlanması)
+	13	Süreç sahibi tarafından artık risklerin kabul edilmesi

Katılım sağladığınız, zaman ayırdığınız ve özen gösterdiğiniz için teşekkür ederiz.

İletişim: tugbametu@gmail.com

BIBLIOGRAPHY

J.B. O'Donnell, & Y. Rechtman. (2005). Navigating the Standards for Information Technology Controls. *The CPA Journal*.

(2004). *COSO ERM.* Comittee of Sponsoring Organizations.

Mapping of CMMI for Development V1.2 with COBIT 4.0. (2006). USA: IT Governance Institute (ITGI).

COBIT 4.1 Control Objectives for Information and Related Technology. (2007). USA: ISACA.

(2012). *COSO Executive Summary.* Comittee of Sponsoring Organizations of the Treadway Commission.

Barnes, F. (2000, l, vol.21, no. 1). Good Business Sense Is the Key to Confronting ISO 9000. *Review of Business Journal, 21* (1).

Debreceny, R. S. (2006). Re-Engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls. *Track 8*, s. 196c. Hawaii: 39th Annual Hawaii International Conference on System Sciences (HICSS'06) .

Hubbard, L. (2005). *Control Self- Assessment: A Practical Guide.* Florida: Institute of Internal Auditors.

McKeever, J. J. (2009). *McKeever CCSA Study System.* USA: Pleier Corporation.

Reingold, S. (2005). *Refining IT Processes Using COBIT* (Cilt Vol.3). ISACA Journal.

Robinson, N. (2005). *IT Excellence Starts with Governance.* Ernst & Young.

Rohitratana, K. (2000, August). Reasons Why Companies Should Have ISO Certification. *Providence Business News*.

Tam, B., L., C., & H, H.-C. (2003). An ISO 9001:2000 Quality Information System in E-Commerce Environment. *Industrial Management & Data Systems, 103*(9), 666–676.

(tarih yok). *Understanding Internal Controls.* A Reference Guide for Managing University Business Practices. California: The University of California.

V.Jovanovic, & D. Shoemaker. (1997). *ISO 9001 Standard and Software Quality Improvement.* University of Detroit Mercy, USA.

Wade, J. (2002, May/June). Is ISO 9000 Really a Standard? *ISO Management Systems Journal*.

Wallace, W. A. (2005). *Internal Controls Guide.* Chicago: CCH Incorporated.

Yong, W. (2010). Information Technology and Enterprise Internal Control. I. E.-P.-S.-E. Conference (Dü.), *Information Technology and Enterprise Internal Control.* içinde

Zhibin, C. (2007, January). On enterprise internal control frame under information technology. *Accounting Research,* 30-37.