Frameworks for establishing and evaluating internal controls: a primer and case study

Denise Dickins
East Carolina University

Margaret O'Hara
East Carolina University

John Reisch
East Carolina University

ABSTRACT

A summary of frameworks commonly used by business organizations to establish and evaluate internal controls is provided together with an example of a recently-implemented Control Self Assessment (CSA) project. Using the CSA methodology in a start-up operation, the process of identifying key business processes, risks to those processes, and controls to mitigate the risks is explained, as is how feedback from the CSA project results in recommendations to improve internal controls. Some of the benefits resulting from CSA, including increased awareness of organizational objectives, development of a sense of employee ownership of internal controls, early detection of risks, and increased effectiveness of the unit's controls are also discussed.

Keywords: Internal control, control self assessment, COSO framework, enterprise risk management, CoBIT

INTRODUCTION

Rapid growth and under-developed financial and operational controls are common characteristics of many start-up operations, including companies, joint ventures, departments, and divisions. Inadequate or improperly working controls can lead to fraud, loss of customers, and even business failure. Managers of start-up operations often fail to adequately address the need for controls because they lack the knowledge of how to address control risk, lack resources to address control risk, or they perceive other issues as being more critical. The manager's dilemma is how to efficiently balance the need for strong controls with the everyday demands associated with running a newly-formed business.

This paper presents several well-known frameworks businesses can employ to establish and assess internal controls, along with a discussion of pros and cons of each framework. It also describes how one implementation methodology, Control Self Assessment (CSA), was executed by a particular start-up operation, and summarizes benefits that may be obtained by other start-ups in need of developing and assessing processes and internal controls. The objective of the paper is to educate readers about the importance of controls, and by discussing an actual CSA project, to shed light on how business processes and controls can be improved by employing a CSA program.

FRAMEWORKS FOR ESTABLISHING AND EVALUATING INTERNAL CONTROLS

A number of frameworks have been developed to assist businesses in establishing and assessing their operational and financial controls. This section is a primer of the leading frameworks. It discusses each framework's pros and cons, and analyzes them in terms of their applicability to and ease of use by start-up operations.[1]

COSO Internal Control Framework

Perhaps the most commonly used internal control framework is the Committee of Sponsoring Organizations (COSO) of the Treadway Commission (COSO 1992). Since the enactment of the Sarbanes-Oxley Act of 2002 (U.S. House of Representatives 2002), external auditors and/or managers of publicly-traded companies with market capitalizations in excess of $75 million have been required to periodically evaluate the operating effectiveness of internal control over financial reporting. In evaluating internal control, SOX requires the use of criteria for evaluation and although not mandated, specifically states the COSO Internal Control Framework satisfies that criteria. Hence, it has become widely used (SEC 2005).

[1] Discussions of the COSO Internal Control Framework, Enterprise Risk Management – Integrated Framework, Control Objectives for Information and Related Technology, and Control Self Assessment are an amalgamation of (1) information available on the Committee of Sponsoring Organizations of the Treadway Commission's website (www.coso.org), the Information Systems Audit and Control Association's website (www.isaca.org), the Institute of Internal Auditors' website (www.theiia.org), (2) various instructional resources including, *Internal Auditing: Assurance and Consulting Services, 2nd Edition* (Reding et al. 2009), and (3) the authors' personal experience working with and implementing the frameworks.

This framework was developed in 1992 as a result of calls by federal regulators (e.g., the Securities and Exchange Commission) and the American Institute of Certified Public Accountants, among others. The COSO Internal Control Framework is designed for managers and companies to establish and evaluate their systems of internal controls. It addresses processes designed to provide reasonable assurance of the achievement of management's objectives pursuant to the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. Figure 1 (Appendix) is a representation of the COSO Internal Control Framework.

The COSO framework suggests that the foundation of an effective system of internal control is a strong control environment, one that can be described as having management and the organization's governing body (e.g., board of directors) committed to competence, integrity, and valuing the assignment of responsibility over internal control. In layman's terms, the control environment is often described as the "tone at the top," which simply refers to how much the people at the top of the organization care about the entity's internal controls.

With this foundation in place, management assesses the risks associated with not achieving its company-and process-wide objectives. For example, if management has established the objective of having a customer product return rate of no more than two percent, what risks exist that could prevent the achievement of this objective? The risks might include receipt of defective products from suppliers, improper manufacturing, or inaccurate product shipping.

In the next phase of the COSO framework, control activities are established to address the identified risks. Management must first determine whether the identified risks should be shared, avoided, reduced, or accepted. In other words, management establishes its appetite for risk. In the product return example referred to above, sharing the risk might mean entering into an arrangement with the company's supplier that any customer returns deemed to be attributed to the quality of the supplier's product, would result in a chargeback to the supplier. Avoiding the risk would mean deciding to exit the line of business. If management elected to respond to the risks identified, then they might establish quality control functions to spot test goods received from suppliers, and to sample production output. Controls could also be established to double check all pulled customer orders prior to shipping. The establishment of control activities also includes consideration of information system general controls (e.g., security, business continuity, and change management) as well as application controls (e.g., information processing) controls. Accepting the risk would mean that management determines that the cost of establishing controls is greater than the cost of customer returns, so the "do nothing" alternative would be selected.

Once established, control activities must be monitored to ensure their operating effectiveness (i.e., that the controls are working) and efficiency (i.e., the controls selected remain cost-beneficial). Monitoring activities might include periodic assessments of the effectiveness of internal controls by managers, internal auditors, and external auditors, and communications between those parties and the board of directors. An important aspect of monitoring is ensuring that changes in the company's external (e.g., competitors, regulations) and internal (e.g., acquisitions, products, delivery methods, systems) operating environments are reflected in changes in risk assessment and control activities.

The COSO Internal Control Framework recognizes the importance of the quality, timeliness and effectiveness of information and communications in ensuring that all significant risks have been identified, the appropriate controls have been established, and those assigned to monitoring can execute their responsibilities effectively.

The COSO framework is very broad, applicable to the effectiveness and efficiency of both operational and financial reporting controls. It is fairly easy to understand and is adaptable to both start-up and mature business operations, though its applicability to more complex businesses (e.g., those with varied operations and complex data systems) suffers somewhat due to its broadness. Proper execution of the COSO framework is dependent on the ability to establish a strong, formal control environment; however, the framework provides minimal implementation guidance. This lack of detailed guidance related to implementation of the framework may make it overwhelming or difficult for start-up organizations to execute. Managers of departments or divisions within organizations may perceive the COSO Internal Control Framework as being too broad or cumbersome to apply to their specific operations.

ERM

The Enterprise Risk Management – Integrated Framework (ERM) was also developed by COSO (COSO 2004). It is a process that is applied across an organization and is designed to help identify risks to provide reasonable assurance that an entity is able to meet its business and financial reporting objectives. Figure 2 (Appendix) is a representation of ERM.

The components of ERM are similar to that of the COSO Internal Control Framework. They include an internal environment which is nearly identical to the COSO Internal Control Framework's control environment. The second step of ERM is objective setting, which consists of establishing desired business outcomes. For example, management may set an objective of having profitable operations, operating in an environmentally-friendly manner, complying with laws and regulations, being financially conservative, or developing a reputation for being a "best place to work."

After setting objectives, the next step in ERM is to identify events, both internal and external, that could prevent the company from achieving its objectives. For example, changes in technology, unforeseen entrants to the market, employee fraud, acquisitions, or interest rate changes could all adversely affect the achievement of the entity's objectives. Each event is then assessed in terms of the controllability of its risk. For risks that are deemed to be controllable, management then determines their response, such as sharing the risk or reducing the risk by establishing appropriate controls.

As with the COSO Internal Control Framework, ERM recognizes the importance of the quality and source of information and communication, and requires that the process be continuously monitored.

The primary difference between ERM and the COSO Internal Control Framework is directional. The COSO Internal Control Framework is depicted as being integrated bottom to top viewing the organization as being a single unit with a single set of risks; ERM is depicted as being integrated across the organization allowing departments or divisions to have different objectives, risks, and responses to risks. A portfolio view of risk is developed at both the divisional or business unit level, as well as the overall entity level. In some ways, ERM might be described as extending the COSO Internal Control Framework and is particularly applicable to more complex businesses.

Like the COSO Internal Control Framework, start-up operations may have difficulty executing ERM due to its broad nature, perceived complexity, and lack of implementation guidance. On the other hand, ERM may also be perceived as being more applicable to operational, not just financial reporting, risks, and may be seen as being more applicable to divisional or business unit level objectives and risks, rather than just entity level objectives and risks.

CoBIT

Control Objectives for Information and Related Technology (CoBIT) was originally developed by the Information Systems Audit and Control Foundation (ISACF) (ISACA 2007). CoBIT is largely aimed at balancing information technology risks and controls applicable to enterprise-wide information systems. CoBIT incorporates most generally accepted worldwide standards and regulations for information technology (e.g., International Standards Organization, COSO, American Institute of Certified Public Accountants, Institute of Internal Auditors - IIA, Government Accountability Office). Figure 3 (Appendix) is a representation of CoBIT.

CoBIT provides for controls across a domain and process framework. The framework consists of a large set of IT processes (e.g., point of sale systems, accounts payable), grouped into four primary domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. Supporting these IT processes are more multiple detailed control activities necessary for effective implementation. The CoBIT framework also addresses specific information objectives such as the quality and security of information, as well as its alignment with the entity's business strategy (i.e., fiduciary role).

Organizations employing CoBIT generally have sophisticated information technology systems increasing the risk that the failure of such systems will result in management being unable to achieve their business strategies and financial reporting objectives. As such, CoBIT is generally not a framework applicable to start-up operations or individual operating divisions.

CSA

Control Self Assessment (CSA) is more an implementation strategy than it is a unique framework. It was formally developed by the Institute of Internal Auditors (IIA) to identify business processes and develop processes and controls to effectively and efficiently address risks associated with those business processes (Tritter and Campbell 1996). CSA is easily adapted to business units, divisions, or functions, and encourages process owners to take responsibility for the achievement of business objectives. Figure 4 (Appendix) depicts the CSA process.

CSA's components align with the internal control frameworks discussed above (COSO, ERM, and CoBIT). The frameworks provide a set of goals and metrics for business processes, and CSA essentially monitors those matrices.

CSA is a method for assuring that an organization's internal control system is reliable. It is a methodology in which employees review key business objectives and processes, identify risks in achieving those objectives, and assess existing controls to mitigate the identified risks. In simple terms, CSA is "preventative maintenance," whereby a review of controls is undertaken periodically to avert potential problems; any noted problems or significant issues are reported and addressed before they happen.

CSA gains insight on existing risks and controls by soliciting information about the business units from employees and managers who have knowledge of the day-to-day operations. Information is usually gathered through questionnaires and surveys, as well as facilitated meetings (Tritter 2000). Facilitated meetings are often viewed as critical to the success of CSA because the rapport helps employees gain a better understanding of business risks and internal controls, and the interaction empowers workers to assess or even design controls. A desirable by-product of this empowerment is an increase in accountability because employees develop a sense of ownership of the controls.

One important aspect of CSA is that it is "employee owned." The key is that employees view this as means for improving their environment. Any weaknesses should be identified and fixed. If employees believe that negative ramifications will arise as a result of for identifying a problem, the CSA is destined to fail. Thus, the CSA must be framed positively to the employees and should not be regarded by employees as additional work (e.g., just one more hoop to jump through to appease management).

CSA's flexibility and guidance provided by the IIA make it easily adaptable to a variety of organizations. Even start-up entities can utilize CSA to determine whether business risks are being properly addressed. The next section describes how CSA was employed to enhance the operating controls of a particular start-up operation.

USING CSA TO ENHANCE INTERNAL CONTROLS

The East Carolina University (ECU) is a public institution with an enrollment of nearly 28,000 students. The College of Business (COB) houses an Exam Proctoring Office (the Proctoring Office) that commenced operations approximately three years ago. The Proctoring Office primarily administers, or coordinates the administration of, exams for students enrolled in ECU's on-line programs. It also works with students enrolled in face-to-face classes when requested by faculty. The Proctoring Office has four full-time equivalent employees. During non-exam weeks, the Proctoring Office administers approximately 35 in-office exams. During midterm and final exam weeks, totaling about three of the fourteen weeks in a semester, the Proctoring Office administers approximately 125 in-office exams. The Proctoring Office also coordinates off-site exams with approximately 600 off-site, unaffiliated proctoring institutions/individuals. This coordination involves approving proctors, scheduling exams, distributing and collecting exams, and resolving a variety of student-specific problems such as assisting students with disabilities. In a given semester, the Proctoring Office helps off-site proctors administer approximately 1,600 exams for students enrolled in the COB's distance education programs.

Key processes of the Proctoring Office are scheduling on-campus exams, administering on-campus exams, returning completed exams to faculty, and coordinating off-campus exams with off-site proctors. As such, the Proctoring Office's key constituents are students, faculty, and off-site proctoring institutions/individuals.

Faced with the challenge of rapid growth in the number of exams proctored, management was concerned that its current controls over scheduling, administering, and returning on-campus exams, and its processes for coordinating with off-site proctors, might be, or might become, inadequate. Accordingly, management sought to gain a better understanding of the effectiveness and efficiency of its controls, and of its constituents' needs.

As a first step, management consulted with individuals familiar with the establishment and evaluation of systems of internal controls. Considering the limited availability of Proctoring Office staff, the lack of any formally documented processes, and the lack of employees' familiarity with control systems, management determined that implementing CSA using a combination of facilitated meetings, surveys, and independent tests of existing controls, best met its objectives.

The project was led by a facilitator independent of the Proctoring Office. The steps identified for execution of the project were: prepare key process memos, evaluate the effectiveness of existing controls, and develop recommendations for improvement in processes and controls. During the initial consultation with employees of the Proctoring Office, the facilitator stressed that the ultimate goal was to improve the operations of the units. Any shortcomings noted during the CSA would not result in punitive assessments of anyone; rather, the control weaknesses would be corrected to enhance operational efficiency and effectiveness.

Process memos detailing the key processes and current controls were prepared based on a series of facilitated meetings with employees of the Proctoring Office. The following is an example of a process memo:

> "Administering Exams
>
> On test day, the student will show up at the designated time, and the proctor will ask for his/her ID, and check the calendar to confirm the appointment. Once confirmed, the student must sign a sign-in sheet which includes his/her name, course, professor, time, and signature.
>
> If the test is to be administered on the computer (e.g., Blackboard), the proctor will enter the required password which has been provided by faculty. If the test is paper-based, the proctor will provide the student with the examination. The proctor ensures that exams are completed in the time allotted by faculty. When completed, the proctor staples any notes to the exam, and puts the completed test folder to return to faculty. Once a student has completed an exam, he/she must sign-out on the sign-in sheet. This process reduces the likelihood that students will say they completed an exam when they did not.
>
> To reduce the likelihood of cheating, the proctor will perform several walkthroughs during the exam and will look for notes or computer clicking (i.e., Googling). Computers are currently open-access (e.g., students have the ability to search the internet while completing a Blackboard examination).
>
> Key controls-
>
> - Upon arrival at the Proctoring Office, the proctor checks student IDs and confirms exam appointments.

- Students must sign a sign-in sheet which includes their name, course, professor, time, and signature.
- During exams, proctors routinely monitor for potential cheating (e.g., inappropriate use of notes and websites).
- If the exam is on Blackboard, proctors enter required passwords provided by faculty.
- Students must complete exams within the time allotted.
- After completion of exams, students must sign-out on the sign-in sheet."

After obtaining an understanding of the key processes and controls in place over those processes, the next step taken in the CSA was to evaluate the effectiveness of existing key controls. Independent tests were made and the Proctoring Office's key constituents were surveyed. In the case of the above example of administering exams, the following independent tests were performed:

"Tests of controls-

- During a high-volume exam period of about one hour, observe students arriving at the Proctoring Office, having their IDs checked, and signing-in and -out.
- Observe whether proctors enter passwords, adhere to allotted exam times, and monitor for cheating.
- Inspect sign-in sheets for five randomly selected days during the semester to determine that sign-in and sign-out procedures are followed.
- Schedule a quiz and arrive at the Proctoring Office during the scheduled time period. Determine whether proctors check ID, verify appointment, require sign-in, monitor cheating, keep to the allotted time, and require sign-out."

Surveys of key constituents included a variety of questions aimed at both evaluating the effectiveness of existing controls and gleaning information on improving the efficiency of controls. Applicable to the "Administering Exams" process example, questions included in the students' survey included:

- "How frequently are you asked to present a picture ID prior to taking a proctored exam?

  Never   Sometimes   Often   Always
  1   2   3   4
- How easy would it be for students to cheat on an exam proctored by the Proctoring Office (or Off-site Proctor)?

  Very Difficult   Very Easy
  1   2   3   4   5
- Please briefly describe any problems you have encountered when taking a proctored exam.

- What suggestions do you have for improving the proctoring process?"

Recommendations for improvement were developed based on outputs of the facilitated meetings, independent tests of controls, and survey results. Again, using the "Administering Exams" process, recommendations included the following:

> "University/Banner Identification Cards should be required for all students taking both on-site and off-site proctored exams (as opposed to other forms of picture identification which are more subject to fraud).
>
> The Proctoring Office should consider implementing a University/Banner ID Card swiping system and eliminating the current paper-based student sign-in/sign-out system. Upon arriving at the Proctoring Office, students would show their University/Banner ID to the Proctor and would be required to swipe-in. Upon exam completion, students would be required to swipe-out.
>
> To reduce issues identified by Off-site Proctors and Faculty, the Proctoring Office should adopt a policy to permit only internet-based exams. Exceptions should be rare and only be at the direction of Management of the Proctoring Office.
>
> Although identification cards are checked prior to a student taking an exam, there is currently no verification to determine whether or not a student is enrolled in the class for which the exam is scheduled. The risk of academic integrity is somewhat heightened when students take internet-based exams as it is possible for a student to schedule an exam for a class in which they are not enrolled, and take that exam using another student's log-on passphrase and password. To reduce this risk, the Proctoring Office should verify students' enrollment in the class for which they are scheduled to take internet-based exams."

The CSA project was completed over a single semester (approximately 15 weeks). The time commitment of management and employees of the Proctoring Office was approximately 24 hours, primarily devoted participation in facilitated meetings, development of surveys, and reviews of survey results. Three constituent groups were surveyed (students, faculty, and proctors). Approximately 4,700 surveys were distributed electronically, and 501 responses were received. Time committed to the project by the lead facilitator was approximately 48 hours, primarily devoted to preparing process memos resulting from facilitated meetings, testing controls, administering and summarizing surveys, and drafting recommendations.

To assess the effectiveness of the project, perceptions of management and the employees of the Proctoring Office were gathered on four questions using a 5-point Likert scale anchored at 1 = not at all, and 5 = very much so. The questions and their results are presented in Table 1 (Appendix).

As depicted in the table, participants have a better understanding of the Proctoring Office's processes and controls after completing the CSA. In addition, as a result of implementing CSA, management and employees of the Proctoring Office learned a number of things of which they were previously unaware. For example, students and off-site proctors prefer using Internet-based exams, a methodology easier and more time-efficient for the Proctoring Office to administer. Students prefer on-line scheduling, a methodology that requires an initial investment, but will save personnel resources in the future. One off-site proctoring location had concerns that were leading to discontinuing service. The Proctoring Office was able to easily address the location's concerns and retain service. Had it not been for the project, the Proctoring Office might not have been able to identify and address the location's concerns.

In summary, CSA was a cost-efficient and resource-efficient framework and technique to evaluate the Proctoring Office's controls and to determine ways that processes and controls could be enhanced as its operations continue to expand.

LESSONS FROM THE CSA EXAMPLE PROJECT

The Proctoring Office's CSA experiences are not unique to its operations. Lessons can be taken from the example project and applied to most any business, particularly those that are in the start-up phase, or those that lack the time and money to complete a full-blown evaluation of their systems of internal control. A summary of lessons learned is described below.

Lesson 1: Routinely evaluating systems of internal control is important as the alternative of not evaluating may lead to a decline in efficiency at best, and a loss of business, at worst. In the case of the Proctoring Office, information was gained to improve the efficiency of operations accommodating increases in the number of exams proctored without additional investments in personnel. Results of surveys also enabled management to identify and address concerns that may have gone unidentified and lead to a loss of off-site proctoring locations.

Lesson 2: CSA-facilitated meetings and constituent surveys are a cost- and time-efficient manner to better understand and identify ways to improve processes and controls. Incorporating the same basic components as the COSO Internal Control, ERM, and CoBIT frameworks, the CSA methodology is easily adapted to the processes and controls of departments, divisions, and start-up operations. The greatest time commitment in the CSA of the Proctoring Office was the preparation of process memos, and the administering and summarization of survey results.

Lesson 3: CSA encourages the participation of process owners, enhancing employees' accountability for business risk and controls. When employees better understand processes, risks, and controls, the likelihood that operations will be effective and efficient is increased.

SUMMARY

This article provided a summary of commonly-used frameworks to establish and evaluate internal controls, and an example of a recently-implemented CSA project. The description of the framework provided the foundation for the CSA and emphasized the importance of internal controls to organizations. The discussion of the project illustrated how business outcomes (e.g., time and money) may be enhanced by a review of the business processes and controls to reduce risk to the organization.

In the example project, the internal controls of an operating unit of a university were examined using the CSA methodology. Employees of the unit first identified exiting key business processes, risks to those processes, and controls to mitigate the risks. Subsequently, questionnaires completed by the employees and other constituents provided feedback on the processes, risks, and controls, resulting in recommendations to improve the internal controls of the unit. The CSA of the unit helps to illustrate some of the benefits of CSA, including increased awareness of organizational objectives and the need for strong controls, development of a sense of ownership of controls, early detection of risks, and increased effectiveness of controls. With these types of benefits, and the relative ease of conducting a CSA, this example may encourage business organizations to consider the use of CSA to strengthen their internal control structures.

REFERENCES

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (1992). *Internal Control – Integrated Framework*. Retrieved October 6, 2010 from www.COSO.org.

______. (2004). *Enterprise Risk Management — Integrated Framework.* Retrieved October 6, 2010 www.COSO.org.

Figg, J. (1999). The power of CSA. *Internal Auditor* 56 (4): 28-34.

Heimbaugh, T. L. (2004). CSA—An integral part of the process. CSA Sentinel Online, IIA Control Self-Assessment Center (February).

Information Systems Audit and Control Association (ISACA). (2007). *COBIT 4.1*. (IT Governance Institute: IL). Retrieved August 26, 2010 from http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf.

Information Systems Audit and Control Association (ISACA). (2009). *CISA Review Manual 2010*. Rolling Meadows, IL: ISACA.

Reding, K. F., Sobel, P. J., Anderson, U. L., Head, M. J., Ramamoorti, S., Salamasick, M. & Riddle, C. (2009). *Internal Auditing: Assurance and Consulting Services, 2nd Edition*. Florida: Institute of Internal Auditors Research Foundation.

Securities and Exchange Commission (SEC). (2005). Statements of SEC Chief Accountant Donald Nicolaisen and Corporation Finance Division Director Alan Beller regarding new COSO Guidance on Section 404 Compliance (October 26). Retrieved October 3, 2010 from http://www.sec.gov/news/press/2005-153.htm.

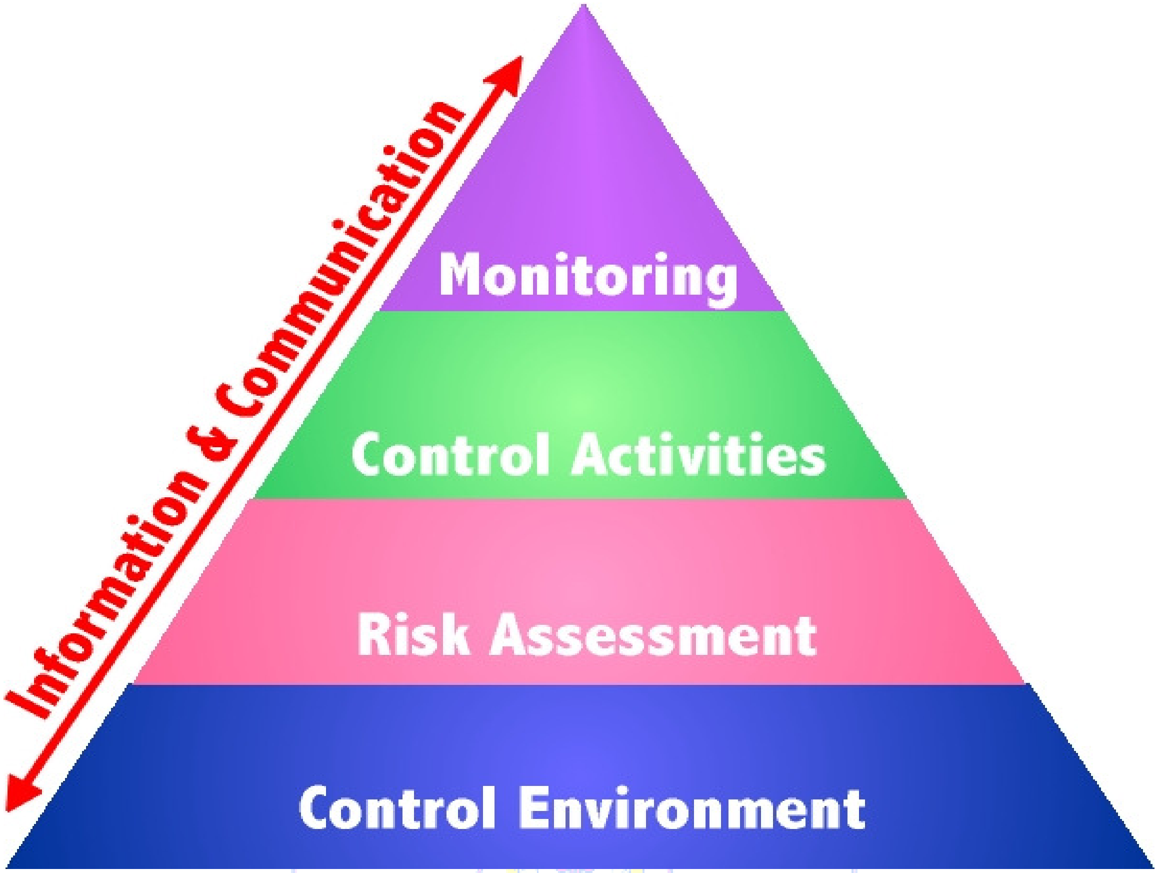
Tritter, R. (2000). *Control Self-Assessment: A Guide to Facilitation-based Consulting*. New York: Wiley.

Tritter, R. & Campbell, L. A. (1996). *Control Self Assessment: Experience, Current Thinking, and Best Practices*. Florida: Institute of Internal Auditors Research Foundation.

U.S. House of Representatives. (2002). The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H. R. 3763]. Washington D.C.: Government Printing Office.

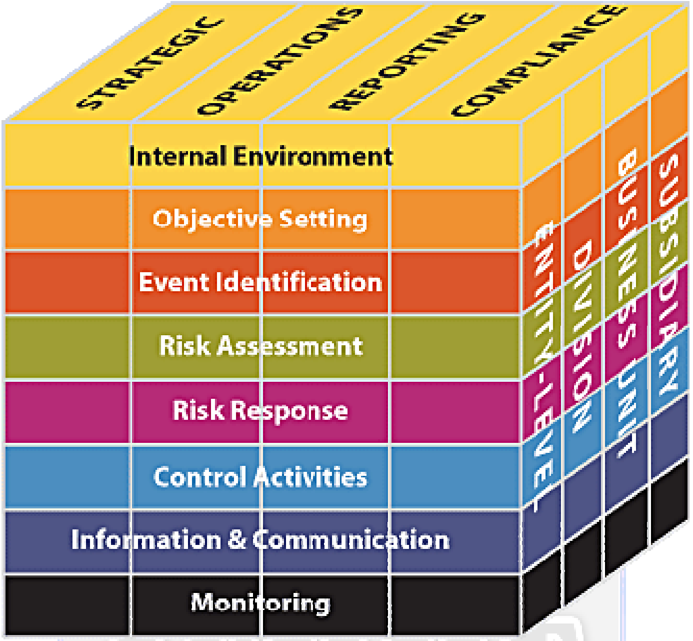
APPENDIX

Figure 1
COSO Internal Control Framework



Adapted from COSO

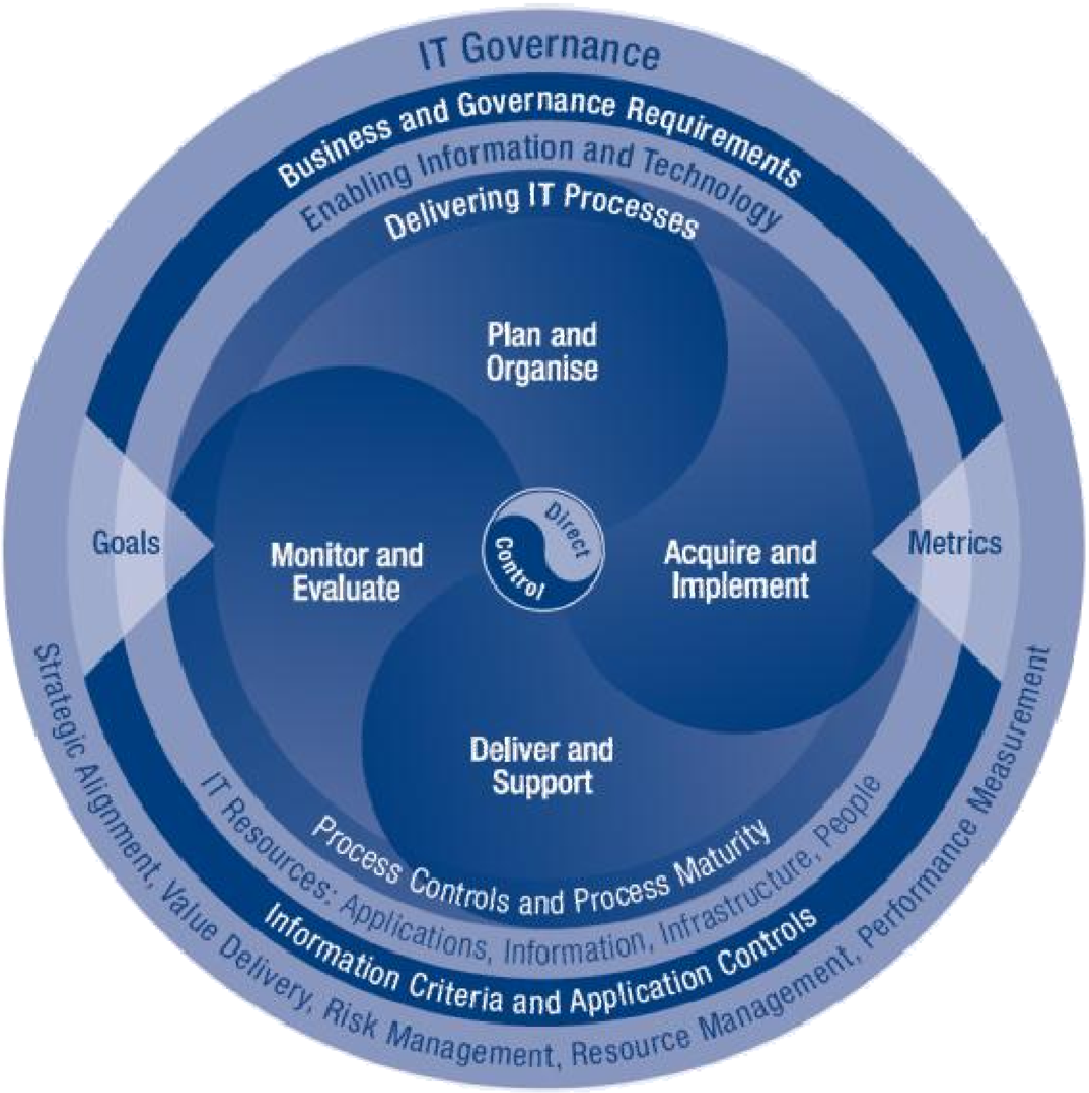
Figure 2
ERM



Adapted from COSO

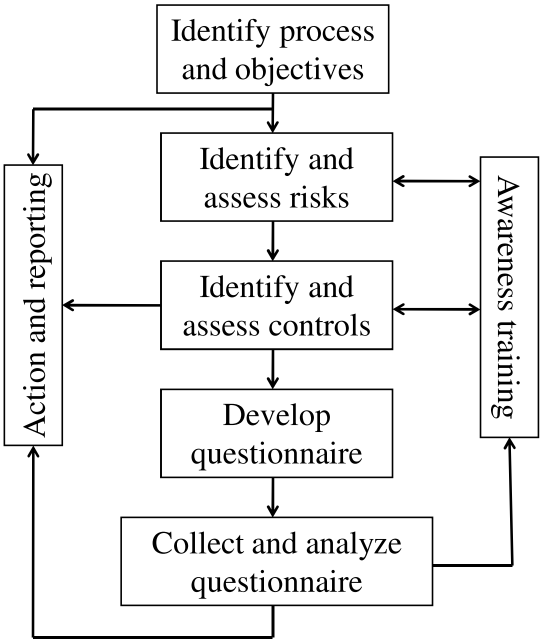
Figure 3
CoBIT

.


IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Monitor and Evaluate
Acquire and Implement
Deliver and Support
Direct
Control
Goals
Metrics
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

Source: ISACA. (2009). Available at: http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx, accessed August 26, 2010.

Figure 4
Control Self-Assessment


Identify process and objectives
Identify and assess risks
Identify and assess controls
Develop questionnaire
Collect and analyze questionnaire
Action and reporting
Awareness training

Adapted from CISA Review Manual (ISACA 2009), Exhibit 1.6.

Table 1
Management and Employee Questions and Responses about the CSA Project

1. Participating in the [project] enhanced my understanding of the Proctoring Office's processes and the importance of internal controls. Mean Score: 4.4

2. Participating in the [project] enhanced my understanding of the importance of periodically testing internal controls. Mean Score: 4.8

3. Participating in the [project] enhanced my understanding of how surveying constituents contributes to testing a process and identification of ways to improve processes and controls. Mean Score: 4.2

4. As a result of participating in the [project], I believe that other departments could benefit from periodic internal audits of their processes and controls. Mean Score: 4.6

Mean scores based on 5-point Likert scale anchored at 1 = not at all, and 5 = very much so.