AICPA CITP Credential Examination Series

Topic: COSO Framework

Presenters: Al Chen and Virginia Collins

Al Chen: Hello, and welcome to the AICPA CITP Credential Examination series. This podcast will assist you in preparing for the examination specifically related to COSO Model Framework topic.

By way of introductions, my name is Al Chen. I am an AICPA CITP credential holder, based out of Raleigh, NC where I am employed by North Carolina State University.

I am joined today by my peer and prestigious colleague, Virginia Collins, also a CITP credential holder, based out of New York City, New York where she is employed by Loeb & Troper. We are pleased to share with you our insight around the COSO Framework.

Now, let's get started. COSO defined internal control as a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievements of the objectives relating to operations, reporting, and compliance.

From this definition, we learned the emphasis of internal control is a process geared to achievement objectives. This is a process consisting of ongoing tasks and the activities, as a means to the end to achieve objectives. It is not an end in itself. It is a system effected by people and their actions at every level of organization to effect internal control. Internal control is able to provide only reasonable assurance to an entity's senior management and board of directors. This is not an absolute assurance because of its inherent limitations in the system.

It is also adaptable to the entity structure. It is flexible in its applications for the entire entity or for a particular subsidiary division, operating unit or business process.

We notice that there is a relationship between the objectives and its strategies. Objectives is what an organization wants to achieve in terms of goals. Strategy will be how an organization plans to achieve their objectives.

COSO internal control framework provides three types or categories of objectives, which allow organizations to focus on different aspects of internal control. To start off with, operating or operation objectives. They are related to effectiveness and efficiency of organization's operations. For example, an organization or company used JIT manufacturing. It's internal control system and the procedures can be established to produce its goods and services sold to customers in a most efficient and effective manner. For example, to ship out the customer's orders within 48 hours upon receipt of the orders from the customers.

Secondly, reporting objectives. This is related to the quality required for internal and external reporting of financial and non-financial information. For example, the control activities put in place to ensure that accounting records, reports capture all business activities for monitoring and performance evaluations.

The last one is the compliance objectives, which related to the adherence to applicable laws and the standards to which the organization entity observes. That will include policy and the procedures established to ensure compliance with mandatory regulations as well as voluntary rules. Mandatory regulations will include examples like OSHA regulations, obtaining patients' consents prior to conducting clinical studies or observing anti-money laundering laws. For voluntary rules, that may include company's environmental sustainability reports that management is willing to share with stakeholders.

We wonder why COSO Internal Control Framework becomes so important because SOX 404 requirements of internal control reports in the company's annual reports. First, management has responsibility for establishing and maintaining adequate internal control over financial reporting. COSO Framework is then used by the management to conduct evaluation of effectiveness of internal control over financial reporting. Finally, the management need to make a conclusion about the effectiveness of internal control over financial reporting at the year-end.

What will be the responsibility of the people in organization have regarding internal controls? First of all on the top, CEO has the primary responsibilities regarding to the internal control systems due to the nature of the position. The CEO is the individual who most directly set the tone at the top. CEO and the CFO must also certify they're fairly present in all material respect, the operations and financial conditions of the company as required by SOX 2002, Section 302.

Board of Directors, on the other hand, provide governance and the oversight in establishing and managing internal control systems. Internal auditors through their independent assessment of the management assertions regarding the design adequacy and operating effectiveness of internal control. They provide an extra level of assurance upon which the board of directors, audit committee, external parties such as the regulators, external CPAs and the shareholder can rely.

For the associates of the organization, they produce or monitor elements of organization's system of internal control. For independent outside CPA and auditors, they do not have responsibility for organization's internal control systems. However, they do contribute independence and objectivity through their opinions. Covering the fairness of the financial statements and the effectiveness of their internal control systems over financial reporting.

In summary, everyone in the organization has responsibility for internal control systems. Internal control should reduce the risk associated with undetected errors and the irregularity, but designing and establishing effective internal control is never an easy and perfect task.

Therefore, there are limitations of internal controls that we should be aware of. COSO pointed out, there are following internal control system inherent limitations. That will include first, the suitability of the objectives established as a pre-condition of the internal control systems. Second, human judgments in decision-making can be faulty. For example, we have human errors and mistakes, misunderstanding, fatigue or stress. Control can also be circumvented by collusion with others among the employees. Management can override the controls already in place. Finally, resource constraints such as the staff size limitations may obstruct efforts to properly segregate duties.

Therefore, these are the limitations that we need to keep in mind to understand that the internal control system does not provide an absolute assurance. Only provide a reasonable assurance of the reliability and the ability to achieve those objectives that we stated above.

Finally, the integrated control framework. We refer to 2013 framework was updated at that time. Those changes are basically reflect the changes in business and the operating environment. For example, the 2013 framework reflects increase reliance and the dependence on IT, information technology, as a part of organization's control activities. 2013 framework also enhance focus on fraud risk assessment, requiring considerations of various types of fraud and the fraud risk responses. Types of fraud include fraudulent finance reporting, possible loss of assets and corruptions.

Internal control framework has also elaborated on the implicit fundamental concept underlying five components that will be articulated in 17 principles.

What are not changing including the core definitions of the internal control as we stated at the beginning. Also emphasize that judgment plays a critical role in designing, implementing and conducting internal control processes. Judgment also plays a key role in assessing into the control effectiveness by the internal auditors as well as external CPAs. In those internal controls framework we have maintained three categories objectives and five components of internal control. Each one of those five components of internal control are required for effective implementation of this internal control process.

Now we're going to hand it over to Virginia to continue the discussion and the elaboration of these five components.

Virginia Collins: Thank you Al. I appreciate that. Just to also talk about some of the changes that occurred from the 1993, the original COSO, which was developed by five organizations, independent organizations. Probably came into prominence when all of the Enron scandals happened and different frauds that occurred. It really put COSO in light in the country and internationally, also, where the benefit of the controls and seeing this framework, and having proper controls would reduce frauds and some of the corporate frauds that were occurring. We really came into prominence then as public companies at that point when the Enron scandal and SOX came into being.

Now, public companies are required to report on the effectiveness of controls as part of the auditor's report. Not for private companies, thank God, which is what I'm in. But they do have a report on controls. It became very important - this framework.

The world is constantly changing. The updating of this framework became very important as Al mentioned with IT becoming prominent. It became a separate principle, actually principle eleven under control activities. It became so important that it became its own principle.

One of the things they were trying to achieve in changing the framework was to update it for current things. They actually changed the cube. If you look at the original cube, the actual control environment was on the bottom. They moved it to the top to really denote how important it is the tone at the top when you had the Enron. They could have had great internal controls, and they probably did. The management overrode them by saying, "Forget that. Do what I say". That became prominent. That control environment on the top of the cube in the new framework became very important piece of that.

Some of the other changes they actually call it monitoring activities now in the new cube, whereas they only had monitoring to show that monitoring is not just one specific step. It's multiple steps that are occurring. That also was a change in the cube.

If you look at the cube, they're interrelated. You have the components, the five components: control environment, risk assessment, control activity, information and communication, and monitoring activity.

The other side of the cube is really your objectives. Okay, I need to have for my operations good internal controls. That becomes important for a company to be successful as a company and meet their strategies and objectives. Then they have their reporting objectives. That's where the CPAs really focus on the audit. We're focusing on their controls over financial reporting. That's an objective. The other objective is compliance. That is in totally increasing daily, legal and regulatory. Can I meet requirements of HIPAA if you're a health care entity? Can I meet requirements of holding personal identifiable information?

One of the benefits of this framework is that you could take this framework and adapt it to different objectives. You can even add your own objectives and the framework would probably work. Here you have controls over operation. You have controls over compliance. You have controls over reporting. Each of those five components can be subject to those objectives.

The other side of the cube is the entity part of it, where you're going to, "I could have a larger corporation with sub units". How you apply it could be different based on the unit. You also want some consistency.

That's the three different sides of the cube. They are interrelated. One affects the other. It's iterative. This whole process is iterative of internal control.

One of the things that the framework really helped with the organization by adding the 17 principles and adding points of focus. The points of focus is 81 points of focus. This is really how you could start to implement this frame work. They've given a lot of information on COSO's website to help companies implement these systems of internal control over these objectives, compliance, financial reporting and operational. There's a lot of guidance. That's what people needed is to be able to how do I implement the internal controls. Technology, as we said, Al had mentioned about fraud became very important in the new framework.

Now we're going to talk about the five components and go through, again, we're from the top of the cube. We're going from the control environment.

The control environment begins with the board of directors. Sometimes, I see this a lot, small organizations do not have board of directors. They could still be implemented by senior management. Someone has to govern the organization and take responsibility for the governance in reporting, in compliance. There still has to be someone doing that. They set the tone at the top. They have the senior level. They have to communicate. Which is start to see how that reaches over to another component, which is information and communication.

These are not just stand alone components, they interact with each other always. It's foundational. This is the foundation. It’s influenced sometimes by the size of the company, your history of your company or your regulatory landscape. Like for instance, the health care organization has a lot of regulation. How their internal controls would work would be much more complex than some smaller organization that's just selling some apparel say for instance. It's going to be a lot less.

The control environment is defined by the standards in the organization: standard processing, the structures to establish an organizational chart. I have given authority for someone to purchase. You’re establishing the overall authority in this area. That's very important. The communication is important.

There are five principles in the control environment. The organization demonstrates a commitment to integrity, very important part of it. People have to have integrity. How do you implement that? That's where you get into the points of focus, where you could say we establish standards of conduct. We have a document that describes that when someone comes on board they sign that document. That's how you start to implement it with the points of focus. You would evaluate if people are adhering to your conduct of ethics. You would address if there's deviations from it. Very important. Again, monitoring, another component. You see that they all interact with each other.

The second principle is the board of directors demonstrates independence from management and exercises oversight over the development and performance. Again, smaller organizations may not always have this but in larger organizations, there's oversight responsibility. The board comes in. They're given information. They're operating independently. They're providing oversight of what's happening in the system of internal control, financial reporting area, and compliance, and cyber security. They should be interested in that also. That's been a real risk.

Management establishes with board oversight structures, reporting lines. You’re establishing how information is flowing in reporting of different items so people are aware of what's going on. The communications could be internal and external.

The fourth principle is a commitment to attract and develop and retain competent individuals. Very important to have the right people on your board of directors. You should always have someone that's a financial expert. You have to evaluate their qualification. You have to have a process in doing that. You have to address it if you do not have enough competent people on board. You develop training. You start to implement control activities to meet those objectives.

And the organization needs to hold people accountable when there's an internal control responsibility. They enforce accountability through structures, authorities and responsibility. They establish performance measures. They consider excessive pressure. Do you have excessive pressure in the organization that may make you override internal controls? This is a very important part of the component because if this doesn’t work, nothing else works. If it doesn’t have the solid foundation, your integrity could be unreliable. It’s a very important component.

The next component is risk and the identification of risk. An entity is subject to many types of risk: there are industry risks, there are economic risks, there are financial reporting risks, there are legal and regulatory risks. For an organization, you have to manage these risks. That’s for the viability of the organization. A risk is a possibility that an event may occur that will adversely affect the achievement of some enterprise objective. Very important to identify those risks.

Risk management is essential part of any organization to meet their strategic objective. In order for an organization to survive, they need to have a good risk assessment process in place, were they identify and analyze risk on an ongoing and iterative basis. Those risks are identified. They do an impact assessment. They say, “What’s the likelihood of this risk happening? What’s my risk response?" I have to respond to risk. I could either avoid a risk by not even doing the activity, I can reduce the risk by taking out insurance and I could share it with someone else that could be insurance also, or I accept the risk and say, "You know, I'm going to take the risk. I’m able to absorb that risk even if it goes wrong".

There's different ways to handle risk. It’s not one particular way. The organization has to evaluate. That process that they go through to evaluate, that’s critical for the survival of the organization.

There’s four principles that are introducing the risk assessment component. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risk. Here’s were communication comes in to play. They have to get information, not only internal risk but external. What're they subject to today? What new law has come into play that they might be subject to? Are they responding to that risk?

Communication, as I said, these five components interact always. All the time. It’s an iterative process as risk assessments cannot be done one time. They must be done continually as new risks are identified. The organization identifies its risk to the achievement of its objectives. The organization considers now fraud risks. That’s been interjected into the new framework. How is the organization recognizing the risk of fraud in their organization.

The organization identifies and assess changes. That’s very important for them to identify where risk could be changing, if they’re responding to things that they need to in the risk assessment process. There’s points of focus on the risk assessment. They consider their tolerance for risk. It includes operations and performance goals. External financial reporting objectives complies with applicable accounting standards as accounting standards changes. Are they making those changes to comply the financial reporting is correct. Again, they may have compliance objective. They have to consider their tolerance for risk.

The risk assessment process is very important. The risk could be from operational, customer satisfaction. Again, applying that cube not just in financial reporting but in my objectives in operation. Am I satisfying my customers? Do I have a right cycle time for producing my goods and getting my processes execution? Do I have a patent? Do

I need to protect it? Do I have the right strategic focus. People? Do I have employee turnover? There’s multiple risk that you can have in an organization through the three objectives. All of that needs to be assessed for the ongoing benefit of the organization.

The next component is control activities, which encompasses: now that I have identified my risk, now I have to actually make sure that …, I have certain objectives I have decided to meet, how do I make sure that I meet my objectives? That’s where control activities come into play. Where control activities help you to mitigate the risk you won’t to meet your objective. Control activities is almost like the negative of the objective. If what I am worried about is my control activity, that my objective of my control activity is to mitigate that risk.

We have risk in IT. Those IT risks we start to put in general computer controls. We put in access controls. We start to implement policies and procedures. We have purchasing. I put into place certain amount, you can only approve this amount, then we have to go to a higher level for dollar amount. These are the control activities that help to meet the objectives to eliminate fraud, for instance. We’ve actually put in a segregation of duty.

The organization must come up with the appropriate control activities and make sure that those control activities are mapping the records of the risk they've identified and the objectives they’re trying to meet. It’s very important. The control activity is how we implement the internal controls after we’ve gone through it. It’s very important part of the component.

Say a fraud risk. We could have some fraud risk and estimates. We could have schemes. We could have people that are working together. We could have some vulnerability in management override. How do we implement control activities over those risks, identification of them and making sure that those control activities are working? These control activities have to be updated. Nothing stays in stone. They are a moving document. Again, as risks are identified we need to have the right control activities that are part of internal control and activities established by the policies and procedures.

I always talk about with our staff the control activities sometimes is the implementation of the policies at the control environment. How they’re implemented at the transactional level. That’s the activity level controls and the control activity’s a very important part of this.

The next component is information and communication. Such an important part. It affects everything. How are we getting information from externally to know what new risk facing the organization? Information and communication up and down the organization. How do we know our internal control is working? How do we know that some of the control environment, the board, is really making sure we value internal control? We communicating that to all members of the organization. That is a critical communication that they care about it.

If management doesn’t show they care about internal control, it’s not going to flow down to the control of activity, to the implementation. When you see that management is serious about it and they communicate that, it helps everything to work appropriately. Any type of thing, even if you want to implement a plan, any kind of new computer system, you need the approval of management on the top. It just doesn’t work. That’s what we found out in Enron. It doesn’t work unless there is communication. That’s a critical communication. Once you have the intention of the top authority in the organization and everyone is clear that that is correct, it works. That’s what I've found in my audit work.

Information and communication, the organization obtains and generates user-relevant quality information. To get quality information today we need IT, which is your control activity. Do we have the right control activities over IT to get that reported? We need internally to realize things are not working, to realize that we have problem, to identify risk. That’s why these components are so interactive. They are not one, you go to the other. They just crosslines constantly.

The organization internally communicates information, including objectives and responsibilities for internal control. You have an organizational chart. They communicated through that. You know through policies and procedure that communication is happening. You know what you’re supposed to follow. They are necessary to support the functioning of internal control.

Some of the points of focus in the information and communication is identify information requirements. And the new COSO, has increased because we need external information a lot more today. We have organizations that we work with outside. We actually use a lot of outside service organization. We have to establish communication with them. How are they processing our information? We look at their SOC logs. We start to get information about what they’re doing. Communication has definitely increased. That’s why the update of the COSO was so necessary as the world was changing and very important.

Monitoring, the last one. Probably it’s one of the most important ones. If you do not monitor the whole system of internal control, it will actually fall apart if it’s not monitored and if you’re not implementing where there are gaps. You will identify where I’m not meeting my objective, that I don’t have enough control activities in place. I’m not meeting my objectives. My risks are increasing. All these components I’ve talked about in one sentence because they’re all interrelated. This continuing iterative process of providing and sharing necessary information and monitoring it. Monitoring it on a consistent basis to be able to identify where the organization is not meeting its objectives and making those changes that are required.

And very important, some of the principles the organization develops and performs ongoing and separate evaluations to ascertain whether the components of internal control are present and functioning. Are they functioning and have to take corrective action? Remember, they changed the wording from monitoring to monitoring activities on the new COSO framework to really emphasize how important it is that monitoring is not a single task. It's multiple tasks that identify where we need to be and where the system of internal control needs to change and update.

One of the things I want to talk about is the scalability for smaller entities. I work for a midsize firm so I hear this all the time. My company doesn’t have any internal controls because they’re small. I said they do, they just maybe don’t communicate it well to you. It may be applied a little differently because it’s just small, but they are doing things that you have to ask sometimes the right question. They may not document everything. But for many smaller entities, they do need an internal control system. It just may be implemented a little differently and to evaluate it may take a little longer sometimes. They also have risks. They need to identify them. They need to have a system of internal control and they usually do. We just don’t always identify it.

Monitoring, people can by-pass monitoring. We have to make sure that in the organization they’re making sure that no one is by-passing the system and that it’s not deteriorating over time. The monitoring is implemented to help ensure that internal control processes continue to operate effectively. When designed and implemented appropriately, the enterprise will benefit because they’ll identify correct problems, finally. They’ll produce more accurate information on a timely basis, which only helps their operations to work better. They’ll prepare accurate financial statements. They’ll provide periodic certifications with assertions on internal control. Some of the points of focus talk about corrective actions, communicate deficiency, and that part.

These components are not standalones. They are interactive. One affects the other affects the other affects the others.

There are some guidance on smaller entities on COSO of how they can implement it. I think that’s important to know they can have segregation of duties, managers can review reports of detailed transactions on a regular basis, and managers can select transaction for review to supporting document. The management, they can establish a whistle-blower program for management override to make sure you have a good control environment. They may have a board of directors. They are information technology. They could use off-the-shelf programs to maybe reduce some of the IT risk. The monitoring activities in the smaller entity, they may have less formal monitoring process, but they should still take credit for the monitoring performance.

I’d like to talk about cyber security. You could take this framework, as I said, and implement it against another objective. The framework works.

So, let’s talk about cyber security. You want to implement some internal controls, we’ve said some things about cyber security. If we take our control environment, does the board of directors understand the organization’s cyber risk profile? Are they informed about how the organization is managing the risk? Even though they’re not IT, the control environment has to consider those risks in cyber security. When you’re applying in the framework to a risk of cyber security, the board of directors need to be knowledgeable about the risk they have. They need to communicate with the IT department. The organization and its critical stakeholders, and the risk assessment process has to evaluate what their compliance objectives are and gather information.

If I have a HIPAA requirement because I’m in healthcare, I certainly have more risk than someone that’s not holding personal identifiable information. So, my risk assessment process would be higher. I established control activities. I’m going to buy cyber insurance. I’m going to reduce my risk. I’m going to implement other activities to reduce-- good general computer controls, good access controls. I’m going to encrypt. These are the control activities you’re actually putting into place.

Then you get information and communication. You get some information on logs. You’re looking at, "When was the last time I was attacked? What caused the attack?" Well, maybe we should be monitoring and saying, "We had a couple of breaches. We need to reassess our risk. We need to implement new control activities". That’s the great part of this framework is that it’s adaptable to other objectives. You can go through the same framework and come up with an internal control over cyber security.

I hope that gave you a good overview of the five components of COSO. How it’s changing. I would imagine it's going to change in the future as the world is bombarded with information. I can’t imagine it won’t change again. It’s good that it changes because our internal control system is changing and the COSO framework has to also change.

On behalf of the AICPA Information Management & Technology Assurance Division, we would like to thank you for tuning in for this CITP exam series podcast on the COSO model framework. This is one in a series of podcasts that the AICPA’s IMTA division is pleased to offer around a variety of topics of importance for the CITP exam. Be sure to check out other podcasts in this series on topics that include: data analysis and reporting infrastructures, data backup and recovery (some of your control activities, by the way), information lifecycle management, service organization controls (that’s your SOC 1 report), internal audit, PCI compliance and HIPAA compliance.

Have a great day.

Disclaimer

This podcast is designed to provide illustrative information with respect to the subject matter covered, and does not represent an official opinion or position of the AICPA or AICPA.Org. It is provided with the understanding that the AICPA and AICPA.Org are not engaged in offering legal, accounting or other professional service. If such advice or expert assistance is required, the services of a competent, professional person should be sought. The AICPA and AICPA.Org make no representations, warranties or guarantees as to, and assume no responsibility for, the content or application of the material contained herein, and especially disclaim all liability for any damages arising out of the use of, reference to, or reliance on such material.