# AICPA CITP Credential Examination Series

**Topic: Internal Audit**

**Presenter: Terry Campbell**

**Terry Campbell:** Hello and welcome to the AICPA CITP Credential Examination Series. This podcast will assist you in preparing for the examination specific to the topic of internal audit. My name is Terry Campbell and I am a AICPA CITP credential holder. I'm based in Bloomington, Indiana, where I'm a clinical professor at Indiana University's Kelley School of Business. There might be more background that we can add but given our limited time, let's get started.

First thing I'll talk about will be the internal audit roles and responsibilities in the IT area, then I'll branch into that IT area, talk about the audit universe, specific audit programs, assessment of IT risk. I'm hoping to get to work paper documentation and the nature and substance of an audit report. We'll conclude with some comments on board reporting, which actually returns us a little bit to the roles and responsibilities.

Internal audit roles and responsibilities are very similar to the external auditor with the exception of the fact that we are not legally obligated to file reports or to sign reports and license for such things, but from the standpoint of working with the audit committee and managing that relationship with the audit committee, our Chief Audit Executive must do that.

So, when we're communicating about the internal auditor, we're talking about the Chief Internal Auditor usually referred to as the Chief Audit Executive. The audit committee, which is a subset of the board of directors will have no employed directors, typically, and that audit committee oversees us.

Our budget, though, comes from the business budget. So, we will have consultation with the CEO, CFO, and the board, and the audit committee regarding budgets and resource allocations. There is a process for the internal auditor to submit the risk areas, the work plan, and the various elements for examination each year and that would go through the audit committee. This is designed to provide a degree of independence regarding the audit activities that we undertake as internal auditors.

Typically, the internal audit staff will be employees. Although, there are instances where the internal audit function is actually outsourced. So, it is possible to be an internal auditor, but actually not employed by the organization, specifically. That's one of the minor nuances of the way the audit profession has evolved and that is the fact that if you are an external auditor for a particular firm, you cannot provide internal auditing services.

But another professional services firm, that is another CPA firm, can be the internal auditor for a client who is not an audit client. It's one of the things to watch for in the independence and objectivity areas, but what we seek in internal auditing in order to provide a valid report when we complete our examination.

So, the internal audit responsibility for IT audits will be to create and implement the overall strategy that's agreed to by the audit committee. We would find this audit

strategy to be the focus of our attention. In fact, the planning process is the most important part of what we're trying to accomplish in the internal audit.

One of the reasons for this audit strategy and audit planning process being so important is that we must attempt to have a formally documented audit universe. This universe is comprised of everything. That's a fairly large statement to make, but once you realize that nearly anything can cause problems in an organization, there is a realization that all processes, people, programs, products, performance, all activities must be subject to audit. It is not that we audit everything, but we must have a universe that is compiled of all of those elements.

As we do that, we realized that we would have to keep up-to-date on the business strategy, the operating environment, the regulatory challenges that we may face, and any other economic or market conditions that would occur. This provides the internal auditor with the broadest possible opportunity for recognizing what needs to be examined, what may need to be examined, and what may be skipped in a particular audit cycle.

There's a significant degree of complexity in this audit universe, and when we start looking at it, one of the things that we may want to examine is how long has it been since the last audit. If it's been an extremely long time since the last audit, we need to at least give consideration to the situation where this may need to be included in the audit strategy of a particular year.

If it was audited immediately prior year, then there may be less need to audit if the rating was satisfactory. Of course, the internal audit includes a number of other elements, such as the internal control systems, the internal operating environment, the external environment, and finally, it concludes with the risk-complexity issue and the value of doing the audit is actually contained in examining the risk of missing something combined with the probability that it is a big deal. Now, we use a big deal not as a technical term, but just for the implications of the audit challenge.

More specific things that we might want to look at again as an internal auditor, we should be extremely cognizant of the internal control system. This is the key thing and we assume familiarity with COSO 2013 as at least one, if not the primary, internal control standard that we would examine.

This allows us then to look at tone at the top, regulatory implications, judgments that have been made where we can take a look at accounting estimates and see if they were sufficiently in line with the mission of the organization, as well as the standards that should be applied.

The internal environment, I think, speaks for itself, but we would, at that time, want to make sure that the organizational, operational issues are in place. Now, the external environment, especially in a changing world as we see in 2017, we need to be extremely current on what's happening in the external environment with so many variables changing simultaneously.

The geographic dispersion intersects our risk area, and we now, I think, are seeing a new aspect enter our risk analysis and that's the degree of automation. There’s substantial research on automation as well as disruption of business models, and

these two things combined make the internal auditor a key player in trying to make sure that their audit universe is up-to-date.

So, if we have an audit universe and we have a business strategy, we should be able to devise an audit strategy that makes the best of these two worlds. This would allow us to make a multiyear audit plan where we might not get to every aspect in every year, but we would have a standard plan that would allow us to cover the processes, the environments, the controls that are taking place and recognize these challenges to provide a proper risk report to the board committee. Again, we would come back to this board committee numerous times.

As we maintain this audit universe, we probably need to be sure that we've got some environmental scanning going on at all times. This again is adding or at least clarifying some of the roles that internal audit has. They should be as they move forward in internal audits, especially internal IT audits, they need to be sure that they are as up-to-date as at least the technology that they're going to be facing and if possible, seeing the horizon ahead.

This suggests that not necessarily a customized audit protocol, but at least a flexible audit protocol is needed. There has to be a number of standard things that we do, but to imagine that we're going to standardize everything in this world is a bit challenging. So, let's be sure that our internal audit programs are in line with any international standards that we may need to take a look at, and that we undertake periodic audits of IT audit; that is, we're auditing the IT audit periodically as needed.

As you can see, many of these things are cost-benefit where we're not quite able to quantify the cost as much as we would like. However, I think it's going to be necessary for us to do as much as we can in standardization in order that we've got consistency across audit, and at the same time, maintain a degree of flexibility that moves us forward in the audit process to achieve our objectives within the budget.

For example, if we take a look at the scope of this IT audit, we have to be at least partially familiar with all the technical controls that we're going to need, all of the administrative controls that we're going to need, and all the physical controls that we're going to need.

This places us squarely in the position of being internal auditor of governance, risk, compliance, almost everything in the organization, and it returns us to that audit universe as the concept. We have a universe. We have to decide which elements of that universe are going to be the focus that we're going to take care of.

In fact, if we go just a little bit further in this, we will see that we would have to build an inventory of possible audit elements that we would want to examine. This again takes us to the multi years. So, I would reemphasize multiyear audit planning within the scope of IT audits across the entire universe.

Now, we have to assume that the audit universe can be organized in a hierarchical way for we can see the connectors from each element of the organization to each other element of the organization. We need to figure out a way that we can do some entity-level controls because they span multiple areas.

Again, we're hunting for commonality. We're looking across a number of entity-level controls that we can examine, that will span different types of internal controls. If we do this, we should be able to gain enough insights to understand the enterprise-wide controls that are used.

We're now trying to move to specific audit programs versus custom audit programs. Again, I think you can tell by the tenor of our discussion is that we want to use the program that is the most cost effective. This obviously is a bit of a challenge but it is the thing that we would be confronted with.

So, for a standardized versus custom audit programs, we want to find as much standardization as possible while leaving the opportunity open for a degree of customization. Standardized audit programs are more than likely available after we have conducted a series of audits and have gained some insights. We are assuming some familiarity with what we've been doing and that we've documented it completely at the level that we want to.

The standardized audit programs typically will have evolved over a number of years and may be examined to make sure that they're still relevant, but the whole idea is to get a standardized program that worked quite a number of times. Custom audit programs by themselves may or may not be needed, but at least as elements of the standardized audit program.

The reason I specify this is because a custom audit program has a significant investment, more than likely elements will be learned while we are doing it that prove that we may not have known exactly what we needed to know and therefore, need improvement.

In other words, a custom program might move us a bit towards a standardized program. I think that's where I would land on the concept of a custom program. The more customization you have, the more expensive it's going to be, and the fact is the more learning that will have to take place, which means the customization will have to be reduced and the standardization increased.

Making an attempt to look at the assessment of IT risk and when we start doing that, I think the elements that we're really concerned with here is trying to figure out an audit methodology that matches up with what we need to accomplish. The assessment of IT risk and the roles and responsibility associated with IT risk assessment, begin and end with the business objective of the firm tied to the control objective of the internal control.

We would then try to identify the controls with the business processes that gives us reasonable assurance that the business objectives will be achieved. Again, we cannot have perfect assurance. All we're trying to do is to get to a degree of comfort with evidence, the business objectives will be achieved.

We can then identify the main function of the IT aspect that we are taking a look at and see where the IT general controls need to be tested. We can then check the process risk and then test for that control objective. After we've done this, one of the things that is really great about the internal auditor is they can step back and think

about what an overview would look like to a reasonable person; that is to anyone that's a constituency looking at this particular control and objective and process.

Then we're going to see if we have an effective testing strategy. We test it and we determine if it meets the test. Or, if it doesn't, then we give a report on the corrective actions that might be needed. Typically, we would find out that we've got some things that need to be changed. What we're hunting for is the overall risk that we face, is the likelihood or probability of an IT process failure occurring and its potential impact.

So, what is likely to happen? What is the probability that something would happen, and what is its potential impact? These allows us to look at each application, each control variable and determine what the risk profile is of an organization, as well as the business unit, as well as just that particular process we may be examining.

We would examine that in some detail and if we've got a control that should remove the likelihood and/or the potential impact, probably misstated remove. It reduces the likelihood of the barrier and reduces the value of the impact is probably the goal that we are seeking.

There is no such thing as absolute assurance and there is no such thing as eliminating risk. So, we would not be able to do that. We may have to devise in the IT risk area, we may have to devise a risk mitigation plan that tells us what to do or at least gives advice on the possible responses we might make. Typically, these responses include risk avoidance, risk reduction, risk sharing, and risk acceptance.

Well, we've taken a look at the universe. We've got some programs that we're going to apply to try to determine what we might want to do. We have examined the possible risk of the IT process failure and its impact.

The primary function of our audit work papers are in fact to document everything that we've done, so that if a reasonable person came along, they would be able to follow what we did. They would be able to see, "Oh, this is why they did it. This is why they said this. This is the documentation." Etcetera

So, when go forward on this, we would assume that these working papers contain all the information. I think in today's world where the implication or the expectation from the PCAOB on the external auditor that that will cascade into the internal auditor. Therefore, documentation, documentation, and documentation. So, that's the primary function of the audit work papers.

We would have our planning, our resources, our timing, and in essence, all the things we worked on so far would all be documented. We would identify key factors affecting all the variables discussed, and we could even have some issues provided from management or the audit committee.

This does begin to tell us that the documentation elements are quite important and quite, I would say, voluminous. Things are going to take on because everything has to be documented, including why we thought something. So, if there's any judgment involved, we want to make sure that that is documented into our audit evidence and our thought processes and so on.

Working papers then serve the support for our report. They help us to conduct and supervise the audit because not everyone is going to read the report or look at the working papers, knows what happened. It allows quality checks to be made and only that it provides an institutional memory of what we did, why we did it, how we did it, and when we did it, where we did it. So, it has all the information. Clearly, the working papers need to contain what we were doing and why we were doing it. The evidence that we use to support our findings and also the evidence that somebody overviewed our work, somebody examined it.

So, we've got the work papers that are telling us something and they should make sure that we end up with a documented story. The final thing that goes with working papers is third party reviews, so these working papers may at times be subject to being included in the internal audit. Therefore, we need to be sure that they are documented properly, edited properly, secured properly, and are available for any type of review that may take place.

If we take a look at that, we pretty well got an idea of the functions and the standard information contained in internal working papers. One final thing, these working papers are not accessible by anyone. They must be approved by the chief audit executive. So, our working papers are not freely available to anyone that might want to see those.

Okay, maybe I didn't specify, but I would defintely want to specify that the prior working papers become a key variable in planning the next audit. We can see what was done, and there's all the details, and we can imagine that what we want to do is find ways to improve it in a certain way.

Now, that we've done what we can to get our universe, we now are going to try to figure out a way to figure out what this audit report has to be. Now, there's several things that come to bear on the audit report that we want to examine. I reckon the number one thing is we want the audit report to be objective and demonstrate a degree of independence, and a complete commitment to communicate the results of the audit work. It should also allow follow-up to see if corrective actions are taken.

I would say the number one thing it needs to be timely. Clearly, it's something that we would want to make sure that we got timely working papers. I think that the policy of most internal audits that I have seen is that a draft report is provided to the area that is being improved or at least audited for their response in case we've got something wrong.

It seems to me that that make sense. You don't give them the right to change the audit report, but if we've missed something or misinterpreted something, it seems only fair that we would provide that opportunity for them. Failure to do that means that you are being a bit more aggressive than probably is needed as an internal auditor. If you're expecting to make progress with the relationships in the organization and to keep a degree of, what would you say, mutual respect regarding the audit report.

Now, information that is contained within this internal audit report goes back to the essence of what we discussed so far and that's the internal audit report containing all of the information necessary to demonstrate that our work has been done properly. We have documented it, the documentation is available if needed, and then we

communicate the results objectively in such a way that management can make a resource allocation decision on corrective action.

I think that's the key phrase that we want to emphasize to the internal audit function regarding the audit report. We've given the information. We provided the evidence. We've suggested corrective action, and the next decision by the audit committee would be to make a resource allocation decision to follow through on the corrective actions or to provide a response back to the chief audit executive.

Technically, the audit report should include the audit objectives, the audit scope, audit methodology is compliance with standards, regulations, laws, management purposes, deficiencies, and recommendations is normally done. Again, I would say that the contents include an executive summary that provide the key findings and the key recommendations upfront and then the evidence is provided subsequent to that.

The distribution is quite interesting because it just doesn't go every place. First, it goes obviously to chief audit executive. This is all occurring after we have an agreement that there's no misstatement of factual elements in the audit report. The auditee may disagree with our findings and our recommendations, but they're not disagreeing with our facts.

We have our facts. We have our interpretation. Internal auditor files that. If there's a dissent from that, then the auditee can file that as well and it goes up the chain of command. Typically, it's going to go to the audit committee first, and then it's going to, possibly, go to the complete board of directors, and then after that, it may come in to a larger discussion where some of the key managers are brought together and something is taking place at that time.

Well, it's an intriguing political process in most situations. Yet, the internal auditor must maintain objectivity and independence. Therefore, the key distribution of that report is to the audit committee. Subsequent to that, others will receive it based on the chief audit executive's permission and or the audit committee, which leads me a little bit to the board reporting, the audit committee that should receive that report.

If I'm not mistaken, I would suggest that the audit committee would distribute it to the board of directors. Of course, this could take place from the chief audit executive based on the request from the audit committee.

It would seem likely that we would not report the audit report more than quarterly, and perhaps not even that frequently. So, maybe we have progress reports of how the audit plan is going based on the audit universe and the audit programs and planning we've undertaken. But it seems unlikely that we're going to be able to get that many audit reports through in a particular year.

The purpose and nature of these reports are to be objective, convincing in their objectivity, actually, and supported by evidence. This should allow us as an internal auditor, CITP, to provide value to the constituencies and the stakeholders in the organization that are most important to the overall controls and the overall process of what we're trying to do.

We've tried to talk about the internal auditor being not an external auditor, but leveraging many of the skillset and attributes of the external audit. We try to give an overview of the audit universe including everything. So, it's a very large universe from which we try to examine what element would be the most important for us to take a look at, that would have the highest likelihood and the highest impact if something goes wrong.

We would use specific audit programs, both standardized and custom to do that, and this would allow us to focus on the risk-reward situation regarding IT. Our working papers are documented probably in more detail than anyone of us in the profession ever thought that we would have to get to in audit work papers.

Nevertheless, that is apparently the path and the pattern that what we're on. So, we need to be sure that we have documented, I suppose, every possible combination, permutation, of why we did something, where we did something, when we did something, what we did, how we did it, up to and including judgment of the internal auditor. Why did we judge this as a less likelihood or a higher likelihood? We should be able to defend that.

The audit report that is summarized from that is typically much shorter, more communicative, so that it can speak to the stakeholders, and should provide an understanding to the stakeholders of exactly what has happened, why we recommend this, and what are the corrective actions to be taken with the ultimate outcome of having the audit committee/the board/the executive committee, whoever the stakeholders are, that would have to provide the resources for the corrective action. If we don't close the loop on corrective action then it probably hasn't done us a lot of good to do an audit.

On behalf of the AICPA Information Management & Technology Assurance Division, this is Terry Campbell. I'd like to thank you for tuning in for this CITP Exam Series podcast on the topic of internal audit. This is just 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, Information Lifecycle Management, the COSO Model Framework, Service Organization Controls, PCI Compliance, and HIPAA Compliance. Thanks for listening.