The meeting was held at the IDOT Handley Building and JRTC in Chicago jointly by video link.

The meeting was called to order at 8:38 AM on April 19, 2017.

The FCIAA working group made 5 recommendations about how to proceed in achieving the objective of establishing a workable benchmark for the appropriate amount of audit coverage under FCIAA. FCIAA states each major system of control must be evaluated once every two years.

1. Seek a change to the FCIAA statute to establish specific categories of major systems of internal control that must be audited at least once in every two year audit cycle.

2. Discussed working with OAG to change the 11 categories by narrowing them down to 5 more broad categories.

3. SAMS Manual change – change the 11 categories enumerated in SAMS Chapter 2 Supplement in hopes OAG would follow suite and begin judging internal audit coverage. One admitted drawback of this method is that it might not be successful. The OAG originally adopted the 11 categories of controls developed by IOC in SAMS Chapter 2 as their benchmark for adequate audit coverage. If the categories were changed in the SAMS manual the OAG could continue to use the same benchmark. If this process it to be successful OAG agreement would be necessary in advance to make it work.

4. Discussed using Administrative Code rules to establish the categories and thereby the amount of coverage that is required.

5. Discussed working with OAG to agree on a benchmark for how audit coverage is judged and how an internal audit chief could determine if they are meeting the requirement.

It could be useful for this discussion with OAG to know what other States mandate internal auditors to do and if they have a similar benchmarking system to determine what audits they must conduct.

If we are going to make a change some chiefs felt we need to update the Statutes as that would be in the most effective way to accomplish the changes we are seeking. The biggest problem with that method is that it is not likely to get done soon since all legislation is in log jam.

A chief asked if we make a change and include risk assessments to determine audits performed will the OAG go after our risk assessment process. During preliminary discussions SIAAB board members had with the OAG they made it clear that as of now they don't typically conduct analysis on the risk assessment process during their audit. They said if the process changed to no longer use the 11 categories and instead was based on the risk assessment then OAG would audit the risk assessment process and if it was found to be deficient it could result in an audit finding. Currently, the OAG does not conduct significant review of the risk assessment process so long as all 11 categories are covered.

One chief suggested we consider using NASACT to find out if other States prescribe what Audits must be conducted each year if the information is not currently available.

Most audit chiefs are open to consider a risk based system using a robust risk assessment instead of just relying on the 11 categories established in SAMS to ensure adequate coverage at every agency. Many chiefs indicated they liked the idea of going to 5 categories so that we can use that as a guideline.

One of the largest concerns a chief noted regarding gaining adequate audit coverage under FCIAA is resources and staffing. Almost every audit function is currently understaffed when compared to historically how many auditors were at the agency. Many agencies have vacant positions that can't be filled due to lack of approval or inability to find qualified candidates.

Chiefs discussed how to address FCIAA coverage under the current process with OAG such as if one audit can cover several categories. We should discuss with OAG that when a risk assessment is done in a professional manner we can determine which agencies need to audit certain systems of control based on the relationship of cost to benefit. Some agencies base their auditable units on functional units or programs and other use facilities or locations to identify auditable units.

Changing Statute is a long difficult process which could take years to complete. If auditors were able to change to a risk assessment based process we are taking an approach that is required under IIA auditing standards to determine what areas are cost beneficial and are needed to audit. We should emphasize the point with the OAG that those standards were encouraged by FCIAA and adopted by SIAAB but we are not using them in the approach to what to audit because we use the 11 categories to identify what to audit.

Could SIAAB develop guidance on the risk assessment process to determine what areas to audit? As part of the risk assessment we need to discuss with OAG risk factors to include and if we can place some reliance on external coverage and lack of findings there. One problem with the external auditors judging the risk assessment process is that they will not know the agency as well as internal auditors. It would likely be very difficult to develop a method that would work equally well for all agencies.

SIAAB could use IIA guidelines to develop risk categories to consider when doing risk assessments. This could be started by the FCIAA work group to be considered by SIAAB.

An IT risk assessment is now being done by DoIT at agencies under the Governor. Revenue and Agriculture have already had one completed. Their tool uses NIST as a basis to benchmark performance. Could SIAAB consider using/developing guidelines on how to do risk assessments? Chiefs agreed that it would be useful for SIAAB should share best practices on ideas that work.

One chief asked, if most agencies have insufficient resources & therefore coverage areas are a problem, why are there not more audit findings for insufficient audit coverage?

It was discussed that in the prior year it has very hard to get legislation done. One example given was the agreement on Governor's Office, Comptroller and members of the General Assembly agreed in principle to extend the sunset date for the FRSB and yet it was allowed to sunset by failure to get the legislation passed and signed in time. FCIAA change would be hard or impossible to get done in the near future.

This is a negotiation process so if we can get a better deal that is less disruptive and we can get some of what we want it would be better to accept that result and in future years consider seeking further change than to take an all or nothing stance and insist that we get everything we want in the first revision.

Break 9:40 – 9:55

Most chiefs seemed to agree that we should continue working with OAG on a framework for moving forward in risk assessment. One chief asked if we could use the current 11 categories and give specific reasons why we didn't audit specific categories.

If we use SIAAB official guidance or guidelines, the OAG may use it as their benchmark in future audits to write findings and/or they may look at other guideline items as audit criteria.

In this process of working with OAG to establish a better benchmark for when sufficient audit work has been completed, it will be a negotiation process and we are looking for middle ground so we can't expect to get everything we want. We may go to fewer categories or a risk assessment that would justify skipping small categories like Petty Cash in some audit cycles.

One chief asked if we would still ask management their thoughts and priorities as part of our risk assessment. Many chiefs currently include this as a part of their risk assessment process.

Since resources must be considered in risk assessment and drive which audits can be done and to what degree we can review the areas selected, how can we reflect insufficient resources in our risk assessment when that condition exists? One way to do this is to do a questionnaire and ask managers where their staff spent most of their time & resources last year. This can reveal major initiatives or changes that may need to be examined as a risk. Then do interviews to follow up on questions for that area.

Chiefs can use the risk assessment process and questions to share common issues where weaknesses are noted in other parts of the agency or other agencies which use the same procedures or have similar functions.

With regard to DoIT, how do we determine where DoIT's responsibilities ends and agencies responsibilities begin? The DoIT Chief of Staff is coming later in the meeting to discuss where that line is and how it will be set in the future.

One possible method for partnering with DoIT when they are conducting audits in an agency is for the agency internal audit function to provide a subject matter expert for the systems to be evaluated so that DoIT can understand and identify the laws and procedures appropriate for the system being reviewed.

When chiefs are preparing their risk assessment and developing their audit plan it is helpful to note in the comments what risk was noted that caused the unit to be audited so that we know why it was picked and focus the audit on that aspect.

As per discussion with OAG we need to discuss why they won't allow internal auditors to rely on their on their audit coverage when we pick our audits. Audit standard 2050 requires that internal auditors consider reliance upon testing conducted by external auditors when determining what audit testing to conduct.

According to one audit chief NASACT reports that 40 of 50 states have adapted COSO as their standard for internal control development and measurement. They also noted it is mentioned in OAG audit guide as a benchmark or authoritative source. COSO is the risk assessment process. Agencies are free to adopt COSO as their standard and implement it at their agency, however if the Comptroller's Office adopts COSO as the mandatory standard and notes it in the SAMS manual then all agencies will be required to adopt it and utilize it for their annual risk assessment process.

FCIAA currently requires an audit of all major systems of control once every other year. One chief wondered if OAG would accept agencies conducting a normal assessment and do 50% of the major systems and when possible other (low risk systems), to ensure highest risk items identified are reviewed every 2 years.

Teammate has a function to allow management to provide information through its "team risk module" which new management can use to learn about their area and where managers can go in and add their own information that internal audit can use for the risk score.

CMS is currently developing a process to gather data through GATA to develop risk assessments for agencies under the Governor through Teammate.

If SIAAB is to develop guidance, we don't want to do a prescribed template. If SIAAB did that it could be perceived as mandatory and may not be adaptable to every agency. Instead we can do an overarching framework or methodology as opposed to procedures which should be done at each agency to fit their own circumstance.

SIAAB has a place on their website where auditors can place ideas, templates or methods that work for their specific agencies to share with everyone else. SIAAB doesn't want to be prescriptive and back people into a corner with guidelines.

If we chose to use the SAMS Manual changes to Ch. 2 and/or supplement one limitation of this method is that it allows two agencies (IOC and CMS) to control the process and content. We should we keep guidance generic and we don't need one or two agency(s)/office(s) controlling the process.

If we chose this method we must understand there are two parts to this: Ch. 2 of SAMS which provides the general instructions and prescribed reporting format for conducting the annual FCIAA internal control certification process and the supplement to Chapter 2 which provides optional questionnaires agencies may use for their risk assessment process.

We could seek changes to SAMS Chapter 2 to give guidelines on the risk assessment and establish the expectation that internal audit activities should conduct formal risk assessments to identify areas for audit coverage.

GATA is now using COSO and Green Book as guidelines for risk assessment agencies are free to use these guidelines to conduct their risk assessment.

One thing that should be kept in mind is that if IOC adopts COSO as a benchmark and establishes a requirement (in SAMS Chapter 2) that agencies must use COSO to evaluate their internal control structure then agencies must do so regardless of what resources are required or what it costs to obtain the copy written materials. It may take a lot of agency management and staff time, and it is currently allowed for agencies who wish to adopt it.

This information was not presented at the meeting but is included in the notes for reference: When considering the cost of implementation, here is a section from the COSO website about sharing their materials:

Use within an Enterprise

- The use of a COSO Publication such as the ICIF within your enterprise requires a separate authorized copy of COSO Publication or license to use the COSO Publication for each individual who participates in the implementation of and/or uses the COSO Publication within your enterprise. Volume purchase discounts are available as is an enterprise-wide license.

- Contact copyright@aicpa.org for more information on the potential of an enterprise license. Copying, reproducing, modifying, loading a COSO Publication including the ICIF into a software tool for your own individual use is permitted. You may distribute the foregoing within the context of performing your job responsibilities; however, a separate authorized copy of COSO ICIF or license to use COSO ICIF is required for any individuals that rely on COSO ICIF to perform their job functions. Under no circumstance may you distribute beyond your enterprise or sell to others without permission or licensure.
- An internal auditor or other employee who has purchased the COSO ICIF ***may*** provide a questionnaire based on COSO ICIF to a business unit in preparation for an internal audit or review.
- An individual ***may not*** make COSO ICIF generally available across the organization for use by others in the performance of their job.Providing COSO ICIF training and education within the enterprise is permitted provided each attendee has a separate authorized copy of COSO ICIF or the enterprise has licensed to use COSO ICIF or written permission from COSO has otherwise been granted.

Every agency will be required to purchase materials for each person who will be conducting the review.

SIAAB could be an avenue to adopt standards for internal control including COSO. SIAAB does not have the authority to enforce the requirement upon management, only internal auditors.

With regard to adopting Green Book – hopefully using that process we would have management become more involved but it is difficult or impossible in some circumstances to require participation.

Another option is to try to get management to go through COSO training and adopt it on agency by agency basis. This would encourage management taking responsibility for and designing a better system of controls.

Do agencies do a risk assessment as a whole? Fraud risk assessment and IT risk assessment. Military affairs got a finding for not doing a risk assessment. Some agencies, perhaps 5 or 6 have gotten them.

You can include that in your annual risk assessment and involved in your meetings with management. So that management will address it and audit in accordance.

The ACFE has a tool for accessing risks and a checklist you can use to access fraud risk. They have more tools for members but there are also tools available for not members.

SIAAB website has a fraud checklist linked that is general guidance. Internal Auditing & Fraud guide is no available through the IIA to help people do these assessments.

The OAG would like to see agencies do a:

1. Fraud Risk Assessment
2. IT Risk Assessment

3. Agency wide Risk Assessment – can be used instead of questionnaires

SIAAB could seek a change through JCAR to establish what is to be determined as a major category under FCIAA

One drawback is if we set an administrative code rule and future rules need to be updated we can't make the change easily. More concerns are who would be the agency sponsor? The most logical agency would be CMS to seek a rule change however the rule would need to establish which agencies it is applicable to for proper clarification.

One question chiefs asked was would the rule change address our objective fully?

Discussion among the chiefs was that the rule adopted would be more likely a one size fits all solution that may not work well for everybody.

Some chiefs felt this would just add to OAG's available criteria and create another mandate for agencies instead of a suggestion that could be used (like other solutions would provide). If we want OAG to use this as criteria it must be prescribed and required. We should be able to use IIA's standards and other guidance like statute as our basis to develop guidance.

Bruce Bullard used to be the contact but it has changed to Jane Clark.

The new QAR Matrix – one agency is now using it and likes it a lot. They feel it is much easier with the new matrix and QAR process

Is there a requirement for agencies to conduct a GAAP process audit this year? No the FRSB no longer exists and the law has sunset. Agencies who wish to evaluate their risks to determine if they should conduct a GAAP process audit may wish to look if forms were late, if a large number or dollar value of adjustments were made or if their reviewer comments from IOC indicate problems with the forms submitted when determining if they should conduct an audit in the future.

The DoIT - Chief of Staff Tyler Clark joined the meeting to discuss the future of audit interaction between the agency auditors and DoIT.

DoIT has been working with CMS Internal Audit closely.

DoIT is a centralized IT agency for those under Governor that became effective 7/1/16.

They are using IGA's at this time but they are moving people under DoIT and keeping many of them physically at their original agencies.

DoIT is trying to prioritize new tech programs and procurement.

They attempted to engage Deloitte on how other states have centralized IA. They are now working on how to develop an internal audit function there.

One way to do is with standards CISO.

They are soon planning to do Rutan interviews for DoIT chief and hope to hire soon.

RSM McGladrey will be doing some work with them to firm up how IA will be done there and co-ordinate with other agencies.

The Executive Order says, DoIT must coordinate all security for IT systems, data and electronic records at agencies.

The MOUs and IGAs in use are pretty broad and it would be good to have service level agreements (SLA) to determine responsibilities for DoIT and agencies. DoIT is at the point of trying to develop them once there is time and staff. They are currently trying to establish something as a baseline for everyone and then customize as needed.

DoIT wants to be agile and determine what they can responsibility provide and ensure they can meet SLA and expectations. Then decide if they are going to need t address things at agency.

ERP – DoIT would like agencies to be involved but the time lines is aggressive and can't be met with early inclusion so lots of people so agencies must pick SME's to represent their interests in the process.

ERP implementation is moving forward - pilot agencies had a real hard time at first but they are working to resolve problems so that each successive phase goes smoother and faster than those prior.

On IT contracts – going forward IT contracts will be under DoIT in future and DoIT will likely sign contracts that provide services do with IT, but there will be input from each agency CIO. Agency specific mission critical contracts may need to be between office and contractor instead of DoIT who will do the RFP and contracting.

DoIT is working on a statewide licensing process on tracking programs. In order to do this effectively chief commented that DoIT must look closely at statutes to be sure they are followed or if the system requires a change then seek statutory change.

DoIT said must look at each situation to see if there is a correct IT solution for it or if non-custom or manual process is best. DoIT realizes IT can't be the best answer to every problem.

Organization of DoIT is as follows: Hardik Bhatt is the statewide secretary of IT then the cluster CIO then the agency CIO. For security issues Kirk Lonbom is the statewide CISO.

Many large agencies have things unique to that agency that will require rework when we get to these bigger agencies and it will make the ERP process more expensive if the program and process is already set in stone.

The process is very complicated. DoIT's rule is don't disrupt critical operations. DoIT is continuing the process begun under Quinn – based largely on Agile process but it isn't actually the original Agile process.

DoIT seeks out these issues and solutions through Directors and cluster CIO's in Quarterly meetings.

Custom service is big for DoIT.

Big systems are hard and we need to expect some bumps along the way.

DoIT's process is needed for modernization of the software and added security is really needed. The State needs to be more responsive and transparent but it is really hard without a budget and they are trying to work with stop gap budget to make improvements.

One chief pointed out that some agencies still have shared services and that function must be assimilated first before the agencies they serve can be added. The public safety cluster is one such area which is tough to address.

ERP – Reconciliations are difficult or impossible and getting OAG to sign off on the audit without those being completed or if they are not done in a timely manner could cause delays for CAFR.

Has there been consideration of the federal mandates that need to be considered in the development of ERP? Also, we will need to re-evaluate the timeline for ERP agencies and when they are finally being added to the system.