

Arkansas Department of Finance and Administration
Office of Accounting-Internal Audit Section (DFA-IA)

Function: Agency Risk Assessment: General Overview Workshop
Location: Highway and Transportation Conference Room
Date: February 2014
Time: 9:00-11:00

Preface

The following narrative is that which corresponds to the PowerPoint Slide show that was presented at the General Overview Workshop February 20, 2014. Several General Overview Workshops were conducted from February 12, 2014 through February 20, 2014 and there were a few minor changes to the slides between these dates. The slide show presented on the last training workshop is the final version and the one posted on the DFA-IA website. Additionally, some of the content of this narrative was not covered in the presentation due to time constraints; so, there may be information noted in the narrative that was not mentioned during any of the presentations.

The purpose of the workshop was to provide a general overview of the risk assessment process for Arkansas agencies, including an explanation of risk assessment terminology. It was designed for those who desired assistance in understanding the risk assessment process, in general. This workshop was not agency-specific, so the examples provided were applicable to various agencies. The training was offered to any employee wanting to gain a basic knowledge of risk assessment.

A handout of a blank risk assessment form was provided for this training (pictured below) and reference was made to it during the presentation. This document can be accessed via our website:

<http://www.dfa.arkansas.gov/offices/accounting/internalaudit/Pages/RiskAssessment.aspx>

- Click the link titled “Blank Risk Assessment and Control Activities Worksheet”
- The file will open in Microsoft Excel
- Click the tab titled “Blank Risk Assessment” at the bottom of the workbook

Risk Assessment and Control Activities Worksheet

Agency: _____ Department: _____ Prepared For: _____
 Activity: _____ Date Prepared: _____

Objective Type	Objectives	Risk Assessment			Address to Manage Risk		Corrective Action Plan
		Significant?	Impact	Likelihood	Control Activities	Significance	How or Additional Control Activity

Management's Conclusion:

1. The control activities are sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objectives (or, if achieving the stated objectives).

2. The control activities are sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objectives, except for the control activities listed as not sufficient in the Major Objectives column. The control activities listed as not sufficient in the Major Objectives column are included in the Corrective Action Plan column along with an implementation date. The corrective action will be sufficient to mitigate the risk when implemented.

3. Some control activities are not sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objectives. Management has not identified any control activities that would be cost efficient to implement in order to mitigate the risk to an acceptable level. Therefore, we accept the risk from the stated objectives may not be achieved.

Table of Contents

	Page(s)
Introduction	
Welcome	1-2
Contact Information	2-5
About DFA-IA	5-8
Presentation Structure and Goal Questions	9-10
Segment 1	
Concepts and Why	11-42
Missions, Goals, Objectives-pgs 12-21, 35	
Risks and ratings-pgs 22-24, 36	
Control Activities-pgs 24-26, 36	
Management Conclusions-pgs27-28, 37	
Corrective Action Plans-pgs 29-31	
History	43-56
Requirement	57-60
Segment 2	
The Components of the Agency Risk Assessment	61-70
The Two-year Cycle-pgs 62-63	
Agency Certification Letter-pg 67	
Agency Introduction letter-pg 67	
Blank Risk Assessment and Control Activities Worksheet-pg 68	
Comprehensive Example/Department of Labor-pg 69	
Financial and Administrative General Risks Spreadsheet-pg 69	
Instructions for updating the risk assessment-pg 69	
Service Bureau Risk Assessment Template-pg 70	
How Agency Risk Assessment relates to Internal Control	71-109
Summary	
Answer Goal Questions	110-111

General Overview Workshop

2014 Risk Assessment Training

DFA – Accounting – Internal Audit

(SLIDE 1)

Introduction

- Welcome to the 2014 Agency Risk Assessment General Overview Workshop
- Contact emails:
 - InternalAuditACC@dfa.arkansas.gov
 - Maggie.Garrett@dfa.arkansas.gov

(SLIDE 2)



**STATE OF ARKANSAS
DEPARTMENT OF FINANCE & ADMINISTRATION
OFFICE OF ACCOUNTING
INTERNAL AUDIT SECTION**

Maggie Garrett, CPA, CIA
Audit Manager

1515 W. 7th Street
Suite 215
Little Rock, AR 72201

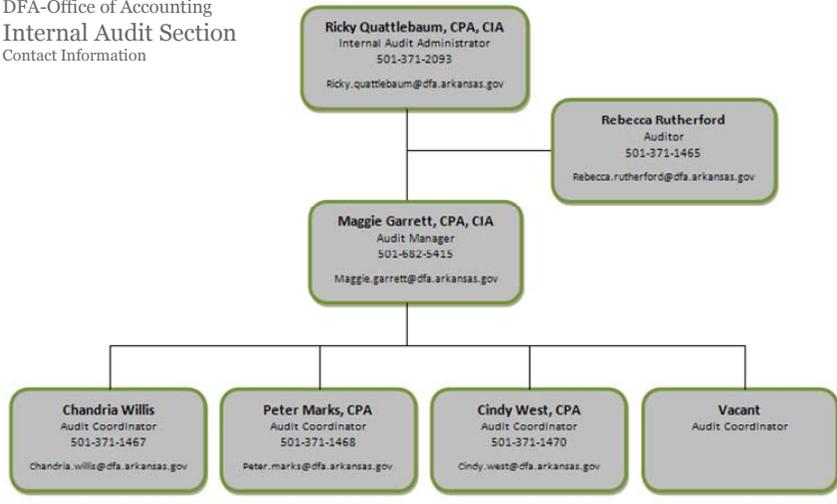
Phone: (501) 682-5415
Fax: (501) 371-1471
Maggie.garrett@dfa.arkansas.gov

(SLIDE 3)

My name is Maggie Garrett and I will be presenting today along with our Internal Audit Administrator, Ricky Quattlebaum. Here is a copy of my business card and as you can see I am the Audit Manager for our office. I have worked for the state for six years and Ricky has been with the office since its creation in 2000. The name of our office is the Department of Finance and Administration, Office of Accounting, Internal Audit Section and as you can tell this is a mouth full. So, I may reference our office for short as DFA-IA or just Internal Audit throughout this presentation.

Organizational Chart

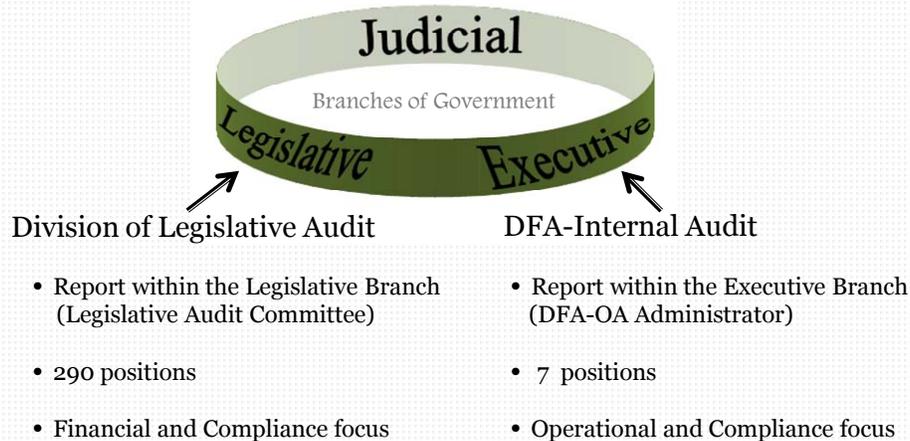
DFA-Office of Accounting
Internal Audit Section
Contact Information



(SLIDE 4)

Here is a copy of our office organizational chart. You can see we have seven positions and on this chart we have all of our names and contact information. Please feel free to contact any of us if you have questions about this presentation or about the Agency Risk Assessment process in general.

Differences between DFA-IA and Division of Legislative Audit



(SLIDE 5)

I would like to start out by telling you about our office. We are sometimes confused with the Division of Legislative Audit, so let me talk about the differences in what we do and what they do.

- Reporting
 - The Division of Legislative Audit reports within the Legislative branch of government, specifically to the Legislative Audit Committee.
 - Our office reports within the Executive branch, specifically to the DFA Administrator of the Office of Accounting.
- Number of personnel
 - The Division of Legislative Audit has approximately 290 positions.
 - We have a total of 7 positions.
- Type of Work
 - Division of Legislative Audit provides the required financial audits for the state, including the CAFR audit, and the A-133 state-wide single audit for federal grants. They also render opinions on the financial statement of agencies. These nature of these audits are financial and compliance.
 - Internal auditors do not usually focus on financial type audits or issue an opinion on financial statements; our work is generally more focused on operations and compliance.

Agency Internal Audit Groups

Agency Internal Audit Functions	Approximate # of Positions
DFA – Office of Accounting	7
Arkansas Department of Correction	4
Arkansas Department of Health	4
Arkansas Development Finance Authority	2
Arkansas Public Employees Retirement System	1
Arkansas Teacher Retirement System	3
Department of Human Services	30
Department of Parks and Tourism	1
Arkansas Department of Workforce Services	5
Arkansas Highway & Transportation Department	20
Arkansas Lottery Commission	2

(SLIDE 6)

We are not the only internal audit group within the state. There are several agencies that have their own internal audit group; here is a list of those that we are aware of and the approximate number of positions of those groups.

Usually internal audit groups work only within the agency. They are considered that agency's internal audit function.

Difference between DFA-IA and Other Internal Audit Groups

Executive Order 04-04

- DFA-IA Application: “This order shall apply to every agency, board, commission, department, division, institution, and other offices of State government located within the Executive Branch of government....”
- “The mission of the Internal Audit Section is to earn and preserve the trust of Arkansans by promoting accountability, integrity and efficiency in the operation of the Executive Branch of Arkansas government.”

Why DFA-IA has been tasked with developing and coordinating Agency Risk Assessment program for the State.

(SLIDE 7)

Our office is considered DFA’s internal audit group; however, we differ from other internal audit groups in that we have authority granted by executive order 04-04 that gives our office the authority to work with all state agencies (and not just within our agency).

The application of the executive order says that it applies to every agency, board, commission, department, division, institution, and other office of State government located within the Executive Branch of government.

It also mentions the mission of our Internal Audit Section and that is to earn and preserve the trust of Arkansans by promoting accountability, integrity and efficiency in the operation of the Executive Branch of Arkansas government.

It is due to this application and mission that we have been tasked with developing and coordinating the Agency Risk Assessment program for the State.

Segment 1

- Concepts and Why
- History
- Requirement



(SLIDE 8)

I will be presenting Concepts and Why of Segment 1 and Ricky will talk about the History and Requirement.

Segment 2

- The components of the Agency Risk Assessment
- How Agency Risk Assessment relates to Internal Control



(SLIDE 9)

For Segment 2 I will discuss the components of the Agency Risk Assessment and how Agency Risk Assessment relates to internal control.

Goal is to answer the following:

1. What is a risk assessment?
2. Why should risk assessment be done?
3. Who should implement risk assessment?
4. How is risk assessment implemented and documented?
5. What are the components of risk assessment?
6. What happens after risk assessment is complete?
7. What is the future of risk assessment for Arkansas agencies?

(SLIDE 10)

Goals of the work shop are to answer the questions: (read slide).

Segment 1

Concepts and Why

(SLIDE 11)

CONCEPTS AND WHY-(Maggie Garrett presenting)

Concepts

- Agency Risk Assessment is a process used by management of an agency to identify, analyze and manage the potential risks that could hinder or prevent the agency from achieving its objectives.

Look at Mission and Goals to help in determining objectives.

(SLIDE 12)

Here is the definition of Agency Risk Assessment as determined by DFA-IA: Agency Risk Assessment is a process used by management of an agency to identify, analyze and manage the potential risks that could hinder or prevent the agency from achieving its objectives.

The first term I want to talk about as it relates to this definition is “objectives”. We want to look at the concepts of objectives and how that relates to the Agency Risk Assessment. Really, the best place to begin is with the concepts relating an objective is to begin with missions and goals. Missions and Goals are not an explicit part of our Agency Risk Assessment document; but, understanding missions and goals can help you in forming an objective. Note that there is an objective column on the blank risk assessment document. Considering the mission and goals can help in recognizing the level of detail that an objective can be in the Agency Risk Assessment document.

The point in ensuring that objectives are identified at the right level of detail (*or with “sufficient clarity” see the COSO definition of the Risk Assessment component of internal control*) is to ensure that risks are sufficiently identified. We will talk more about risks later in the presentation, but for now, understand that the purpose of forming proper objectives is to be able to cover all the risks related to those objectives. The level of detail of the objectives within an Agency Risk Assessment, ultimately, is determined by management of the agency; however, the level of detail of objectives that is in common practice (per our research), is what we will demonstrate within this presentation.

Following are two examples of an Agency Risk Assessment with one showing a broader objective and the other showing objectives at a more detailed level.

Example 1

Objectives	Risks
To ensure payroll is processed accurately and timely.	Risk #1
	Risk #2
	Risk #3
	Risk #4
	Risk #5
	Risk #6
	Risk #7
	Risk #8
ETC.	ETC.

Example 2

Objectives	Risks
To ensure data related to timekeeping is entered into AASIS accurately and timely.	Risk #1
	Risk #2
	Risk #3
	Risk #4
	Risk #5
	Risk #6
To ensure personnel actions are entered into AASIS accurately and timely.	Risk #7
	Risk #8
ETC.	ETC.

Assume that Risks #1-#8 are the same in both Example 1 and 2 above—the risks are not written in detail because it is not important for the point that is being made; just envision that they are the same, meaning Risk #1 in Example 1 is the same as Risk #1 in Example 2, so forth and so on.

For Example 1 and 2 above the same risks were identified even though the objective in Example 1 is broader than those in Example 2 (assume that the agency was able to adequately identify a complete list of risks). What is shown is that an agency can identify all significant risks in both cases; however, according to common practice it is the level in Example 2 that will allow the most efficiency in identifying risks and agencies that use this level will be less likely to overlook significant risks.

With that being said, if agencies have already formed objectives (from prior agency risk assessments) and management has determined that all significant risks have been identified, then it is not necessary to re-work the objectives.

Be aware, however, if objectives are too narrow, then that would decrease the efficiency of identification of risks. If an objective can only have one risk associated with it, then it is likely that the objective is too narrow.

So let's look at missions and goals and get a better understanding of the level of detail that is recommended.

Concepts - Mission

- Usually stated in a mission statement
- Very broad

(SLIDE 13)

A mission is usually stated in a mission statement. These statements will be very broad in the sense that it won't go into the details of the day to day activities to achieve the mission, but it is specific in stating the purpose of the mission.

Concepts - Mission

Examples

Mission: To protect and improve the health and well-being of all Arkansans.
(Department of Health)

Mission: To live a happy, fulfilling life.
(Personal)

(SLIDE 14)

Here are a few examples (read slide).

Concepts - Goals

- Big picture in how to accomplish the mission
- Something that you try to achieve
- Long-term

(SLIDE 15)

Goals are the next step down, and are not as broad as a mission. Goals are the big picture in how to accomplish the mission; they are something that you try to achieve. Goals are considered to be long-term.

Concepts - Goals

Examples

Mission: To protect and improve the health and well-being of all Arkansans. (DOH)

Goal: To provide appropriate and up-to-date technology.

Goal: To utilize human resources.

Mission: To live a happy, fulfilling life. (Personal)

Goal: To retire at an active age.

Goal: To stay married.

(SLIDE 16)

Here are some examples of goals (read slide). So we have a mission and we have goals that we set to accomplish that mission.

Concepts - Objectives

- Viewed as a “result” to achieve
- Measurable
 - Time frame
 - Dollar amount

(SLIDE 17)

Objectives are the next level down from goals. They are what we put in one of the columns of the Agency Risk Assessment form.

Objectives are viewed as a “result” to achieve and are more like short steps in achieving a goal. Objectives are measurable (within a specific time frame) and more detailed than goals.

Objectives

1. Should, in a broad sense, be worded as a “result” that is expected to be achieved.
What does “result” mean, how do you word an objective so that it is a result that is expected to be achieved? One trick to doing this and we’ll talk about this in the Control Self Assessment class is to begin the objective with the word “To” or “Ensure”. So “To provide” or “Ensure that” employees....
2. Should be measurable.
An objective is measurable when it covers a specific time frame or mentions a particular dollar amount.

For most Agency Risk Assessments we have not pushed for the objectives to specify a certain time frame. We assume that the time frame is for a year. If you find that you are having trouble delineating between an objective and a goal, because that can be a fine line, then you can usually determine that by the measurement factor. If it’s not really measurable, then it is most likely a goal rather than an objective.

Let’s look at some examples of objectives.

Concepts - Objectives

Examples

Mission: To protect and improve the health and well-being of all Arkansans. (DOH)

Goal: To provide appropriate and up-to-date technology.

Objective: To provide employees with local area network and access to the internet (for the year).

Goal: To utilize human resources.

Objective: To hire qualified employees (throughout the year).

(SLIDE 18)

Here are some examples of objectives (read slide).

- Note that “(for the year)” and “(throughout the year)” are in parenthesis in the slide, that was just put that there for the purposes of this presentation to show that the examples are measurable. It is optional to include the time measurement value on objectives within your Agency Risk Assessment (and if the option is to include it, then realize there is no need for the parenthesis).

Concepts - Objectives

Examples

Mission: To live a happy, fulfilling life. (Personal)

Goal: To retire at an active age.

Objective: To save \$20,000 this year

Goal: To stay married.

Objective: To say “I love you” at least once a day to my spouse.

(SLIDE 19)

Here are some additional examples of objectives (read slide).

- Note only one objective per goal was listed in these examples, but in reality there would likely many objectives for each goal so keep that in mind.

This slide has an example of an objective with a dollar value measurement.

So, this gives you an idea of the level of detail that an objective can be, and again, the level of detail is important because it is that which will allow for efficiency in identifying risks.

- Note consider the time measurement for the last objective (To say “I love you” at least once a day to my spouse) is for a year. So, the result would be at the end of the year I want to have said “I love you” each day. There could be many risks identified with this objective.

Concepts - Objectives

- Agency Risk Assessment is a process used by management of an agency to identify, analyze and manage the potential risks that could hinder or prevent the agency from achieving its objectives.

↓
Objectives are to be achieved.

(SLIDE 20)

Here is the definition of Agency Risk Assessment again (read slide). At this point, let's talk about the word "achieving". Objectives are to be achieved.

Concepts - "achieving"

If objectives are not achieved, then the risk that the goals and the mission are not achieved can occur.



(SLIDE 21)

This slide demonstrates how objectives, goals and the mission relate.

And what I want to point out is that we want to achieve the set of objectives in the specific time frame so that we achieve our goal so that in turn we achieve our mission.

What happens, if you don't achieve an objective or more than one objective, then you run the risk that you won't achieve your goal or your mission.

So we focus on achieving objectives.

Concepts - "achieving"

Recognize that there is a difference:

- What it takes to achieve
- Capability to achieve

(SLIDE 22)

Consider this when thinking about achieving an objective:

There can be a difference between what it takes to achieve an objective and your capability of achieving the objective.

Concepts - "achieving"

EXAMPLE

Mission: To live a happy, fulfilling life. (Personal)

Goal: To retire at an active age.

Objective: To save \$20,000 this year

- What it takes to achieve: \$20,000 this year

\$20,000 is the "result" that I want to achieve by the end of the year.

(SLIDE 23)

For example, take the goal of retiring at an active age. One of the objectives I listed was to save \$20,000 this year. This is "what it takes" this is the result that I want by the end of the year.

Concepts - "achieving"

EXAMPLE

Mission: To live a happy, fulfilling life. (Personal)
Goal: To retire at an active age.
Objective: To save \$20,000 this year (What it takes)

- Capability to achieve

Capability includes:

Resources, policies, procedures, processes, etc. and the design of such.

Best practice to determine capability is to:

Consider the negative factors (risks) that could affect capability and by determining how to deal with those risks, by default, measurement of the capability to achieve will occur.

(SLIDE 24)

Now let's determine my capability.

When I say capability I mean my resources, my policies, procedures, my processes. The way that I design my processes is within the definition capability.

Standard practice, to determine capability, is to start with the consideration of the risks and then by considering how the agency would handle those risks by default the resources, policies, procedures, processes and the design of such will be considered as well. Thus, by considering the risks and how to deal with those in essence is an efficient way to measure your capability.

Concepts - "achieving"

EXAMPLE

Mission: To live a happy, fulfilling life. (Personal)
Goal: To retire at an active age.
Objective: To save \$20,000 this year (What it takes)

- Capability to achieve

Risk: Gas prices increase

Need to consider the likelihood and impact of increasing gas prices, this type of inflation would have an effect on the calculation of what the savings for retirement can realistically be for the year. (Inherent Risk)

(SLIDE 25)

So, since it is best practice to consider the negative factors first, I have come up with a risk for my example. It is the risk that gas prices increase. I need to consider this type of inflation within my calculation of what I'm going to be able to realistically save for the year.

Notice on the blank Agency Risk Assessment document that the next column after objectives is the risk column.

The likelihood and the impact of increasing gas prices would play a large part in how I would assess this risk and in turn consider it within my calculation of what I will be capable of saving for the year.

Also, note on the blank Agency Risk Assessment document that the columns after risk are significance/impact and likelihood rating columns.

I would consider the likelihood and impact of the "inherent risk". To consider the inherent risk of gas prices increasing I would do research on what was expected in the future, for the time period of my objective (which is a year), and determine how to deal with this risk. So, for example:

- If I determined, through my research, that the forecast was that gas prices will decrease over the next year then the likelihood and impact of the risk would be rated low and small respectively. In other words, if gas prices are going to decrease then the likelihood of the risk occurring would be low. And if the risk does occur it might impact my calculation for what I am capable of saving to be around 10 cents at the most, which would be a small impact as far as I'm concerned.

- On the other hand, what if through my research I determined that the forecast was that gas prices were going to increase by \$2.00 a gallon? In this case, I would consider the likelihood of the risk occurring as high and the impact as large, or in dollars I would interpret that to impact my calculation by \$2.00 per gallon of all the gas that my family uses.

So that's how I would consider the likelihood and impact of the "inherent risk" that gas prices will increase.

Concepts - "achieving"

Example
Objective: To save \$20,000 this year (What it takes)

Risk:	Consider <u>likelihood</u> and <u>impact</u>	<u>Capability to achieve</u> Describe capability of dealing with the risk that gas prices will increase reflecting the determined likelihood and impact.
Gas prices increase	Consider <u>likelihood</u> and <u>impact</u>	Describe capability of dealing with the risk that gas prices will increase reflecting the determined likelihood and impact.
aka: "Control Activities" - the description of the capability to achieve.		
Other risk	Consider <u>likelihood</u> and <u>impact</u>	Describe capability of dealing with the risk reflecting the determined likelihood and impact.
So forth and so on...		

(SLIDE 26)

Remember, we were in the process of measuring my capability to save \$20,000 this year. So, I have considered my risks, one of which was gas prices increase. Realize that we need to consider all negative factors or risks that may affect the achievement of the objective, but due to time constraints for the purpose of this presentation, I'm only going go through one risk. Understand that there are many risks to this objective that should be considered.

For each risk I have considered the likelihood and impact of the inherent risk.

Now, I need to describe my capability of dealing with the risk that gas prices increase. This description of the capability to achieve for each risk is also known as "Control Activities". You will notice on the blank Agency Risk Assessment form that the next column after the ratings column is titled "Control Activities". Control activities are the description of how risks are dealt with or "mitigated".

So, in essence, if I take into consideration all of the descriptions of how to deal with all of the risks for this objective, overall I will be measuring my capability to achieve the objective.

Concepts - “achieving”

Example:

Capability to achieve: can save \$3,000

If I don't change anything I will realistically be able to save around \$3,000 for the year.

(SLIDE 27)

I have analyzed my capability to achieve the objective and determined that if I don't change anything I have the capability to save \$3,000 for the year.

Concepts - Reasons **why**

1. **An agency should conduct Agency Risk Assessment to use as a tool to determine the capability it has to achieve its objectives.**

(SLIDE 28)

Let's pause from our example for a second, if you will remember, the topic we are covering was titled "Concepts and Why". So, I want to point out at this time one of the reasons of why Agency Risk Assessment should be done.

An agency should conduct Agency Risk Assessment is to use it to determine the capability it has to achieve its objectives.

Concepts - “achieving”

Example:

What it takes to achieve: save \$20,000

Capability to achieve: can save \$3,000

Next step: Make a [comparison](#).

(SLIDE 29)

Back to the example:

The next thing we need to do, and what may be just stating the obvious, is that we need to compare “what it takes” to the “capability”. Now this comparison is easy for this example because it’s dollar values, but when it comes to comparing those objectives that are measured in time are sometimes not so easy to compare, in fact it can be one of the hardest parts of the process.

Concepts - "achieving"

Example:

What it takes to achieve: save \$20,000

Capability to achieve: can save \$3,000

With no change, is the capability to achieve the objective:

SUFFICIENT OR *NOT*SUFFICIENT

?

(SLIDE 30)

I need to ask the question "is the capability to achieve the objective sufficient or not sufficient?"

In this case it is not sufficient. This comparison tells me that if I don't change something I'm not going to reach my objective. (I will be working for as long as I live.)

Concepts - "achieving"

Example:

What it takes to achieve: save \$20,000

Capability to achieve: ~~can save \$3,000~~
 cap: can save \$20,000

Next step: Corrective action plan.

(SLIDE 31)

What do I do now? I look at how I can make changes so that I can reach my objective. I need to come up with a "corrective action plan". I need to increase my revenues or decrease my expenses or probably in this case a combination of the two to be able to reach my objective.

I need to put into action what it takes to make myself capable of achieving my objective.

Concepts - "achieving"



If this is not done, then how would you know if changes need to occur?

In many cases, it is not known until it is too late.

"Uh oh!"

(SLIDE 32)

Here's a question: If I don't determine "what it takes" and I don't measure my "capability" and then compare the two, how would I know that I needed to make changes so that I can change my "capability" to do what it takes to achieve this objective? How would I know?

I wouldn't, not until it's too late to do anything about it. If I didn't go through this measurement and comparison process then I would get to the age I want to retire and look at my bank account and say, "Uh oh, that's inconvenience, if only I had known sooner".

Are there any of you that work for an agency that has gotten to the point of an inconvenient "Uh oh"?

Concepts - Reasons **why**

1. An agency should conduct Agency Risk Assessment to use as a tool to determine the capability it has to achieve its objectives.
2. **An agency should conduct Agency Risk Assessment to have reasonable assurance that the agency's objectives will be achieved (so that a major "Uh oh" will not occur).**

(SLIDE 33)

That brings us back to the reasons why Agency Risk Assessment is done.

A second reason that an agency should conduct an agency risk assessment is to give reasonable assurance that the agency's objectives will be achieved so that a major "Uh oh" will not occur.

Concepts - "achieving"

Question:

Will the **capability** be the same tomorrow as it is today?

Answer:

Depends on **changes**

(SLIDE 34)

Let's go back to the example.

Question: Will my capability be the same tomorrow as it is today? Maybe, maybe not. Tomorrow's circumstances may change. Tomorrow is a new day.

In theory, I have made changes to my policies, procedures or processes with the corrective action plan, but how do I know that they work in tomorrow's circumstances?

I won't unless I do the measurement and comparison tomorrow.

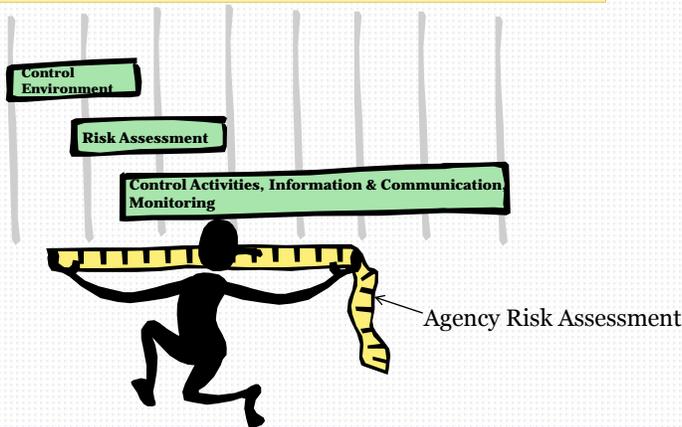
Any time anything changes that could have an effect on what it takes or the capability where it would make the capability to achieve the objective less than what it needs to be, I need to be able to sit down and think about if I need to make any changes so that I can be reasonably assured that I will have the capability to obtain my objective; and the sooner the better. The sooner that I can make changes, the better chance I'll have at increasing my capability.

But who has time to measure and compare the capability of every objective every day? No one. That is not feasible.

Wouldn't it be nice if there was some kind of system I could put in place to alert me if my capability starts to fall short, something that does this measurement and comparison automatically. Would it not be nice to have an alarm system in place?

Concepts - "achieving"

SYSTEM OF INTERNAL CONTROL



An "alarm" system that can detect **changes**.

(SLIDE 35)

Good news, an alarm system does exist that management can put into place. It's called a system of internal control. We will go into great depth about a system of internal control in segment 2 of this presentation.

But for now, know that if an agency has a strong system of internal control then changes that could affect the capability of an agency being able to achieve its objectives will be identified immediately, new risks may evolve as well. These changes should be reflected on the Agency Risk Assessment document as they occur; as well as, any changes to the control activities or new corrective action plans.

As you can see in the slide, there is an arrow from the words "Agency Risk Assessment" to the picture of the measuring tape that the person is holding. This is to emphasize that the Agency Risk Assessment can be used as a tool to measure the system of internal control. I will expand on this concept in segment 2 as well.

Concepts - Reasons **why**

1. An agency should conduct Agency Risk Assessment to use as a tool to determine the capability it has to achieve its objectives.
2. An agency should conduct Agency Risk Assessment to have reasonable assurance that the agency's objectives will be achieved (so that a major "Uh oh" will not occur).
3. **An agency should conduct Agency Risk Assessment to measure the system of internal control (to ensure that the alarm system is designed to work properly).**

(SLIDE 36)

This brings us back to the reasons why:

A third reason to conduct an agency risk assessment is to measure its system of internal control, in other words, to ensure that the alarm system is working properly.

Concepts

Example

Mission: To protect and improve the health and well-being of all Arkansans. (DOH)

Goal: To utilize human resources.

Objective: To hire qualified employees (throughout the year).

Determine “what it takes”

- *Correctly determine through the application process if applicants meet set education and experience qualifications to perform job duties.*
- *Conduct appropriate interviews that would determine if an applicant is qualified.*

(SLIDE 37)

Let's do another quick example from an agency perspective.

First, we want to measure or determine what it takes (read slide).

Concepts

Example

Measure “capability”

(To measure this consider the risks)

Risk:

Applicant is hired whose credentials do not meet the education and experience qualifications.

Consider likelihood and impact (inherent risk)

Capability to achieve

(aka: Control activities)

HR Manager screens the applications to ensure that applicants are qualified. Manager verifies credentials with references.

So forth and so on...

(SLIDE 38)

Next, let's talk about the capability to achieve this objective.

Remember we discussed earlier one of the easiest ways to determine capability is to consider the risks or negative factors first and then determine if the agency can handle mitigating the risk. So for this objective, here is an example of a risk (read slide).

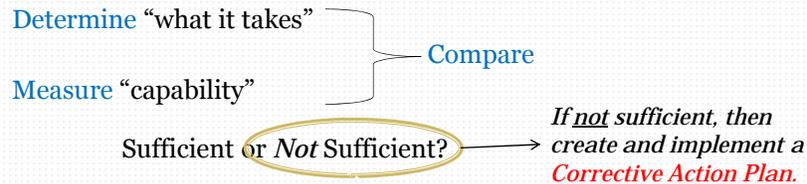
Realize that there should be more than one risk identified with this objective, but due to time constraints of this presentation we will only look at one.

The next step is to rate the risks. Keep in mind we are rating the inherent risk. This is the risk without consideration of control activities.

- For example, for this particular risk you might consider factors such as the economy, so if unemployment was high and jobs were scarce, then how likely would it be for applicants to falsify an application? What would be the impact if an applicant was hired that was not actually qualified? Remember...this is before control activities are even identified. These ratings are considered without control activities in mind. These ratings are for the inherent risk.

Next, we need to think about whether or not the resources, procedures, processes, etc. that we have in place will either keep the risk from happening or at least notify the right people that the risk has occurred and to do something about it. That means that we need to think about the “control activities” that have been put into place to mitigate the risks. By doing this for all significant risks we will have considered that which needs to be considered when determining the capability of achieving an objective.

Concepts - "achieving"



Management conclusions for each risk should be done.
Then, an overall management conclusion can be determined.

(SLIDE 39)

What's next? We compare what it takes to the capability. If it is determined that the capability to keep the risk from happening is not sufficient then a corrective action plan should be put into place to change the policy, procedures, processes so that your agency's capability is where it needs to be.

Notice in the blank Agency Risk Assessment form that there is a column titled management conclusion. The sufficient or not sufficient determination relates to that column. This is the column where management would place an "S" for sufficient or "NS" for not sufficient depending upon the result of the comparison that was made.

I want to also point out that for the last example where I determined that my capability to save for retirement was \$3,000 that we didn't go through the comparison of determining management conclusions for each risk, but in reality, management should make the sufficiency rating for each risk and then, also, have a management conclusion about sufficiency overall.

Notice at the bottom of the blank Agency Risk Assessment document that there are three paragraphs. This is where management would make an overall rating related to the sufficiency of all the control activities in place for the activity. So realize that there are two types of management conclusions: one for each risk and then one overall for each activity.

Concepts - Reasons **why**

1. An agency should conduct Agency Risk Assessment to use as a tool to determine the capability it has to achieve it's objectives.
2. An agency should conduct Agency Risk Assessment to give reasonable assurance the agency's objectives will be achieved
(so that a major "Uh oh" will not occur).
3. An agency should conduct Agency Risk Assessment to measure the system of internal control (to ensure that the alarm system is designed to work properly).

(SLIDE 40)

Back to the reasons why to conduct Agency Risk Assessments.

1. Use it as a tool to determine the capability of an agency.
2. Give reasonable assurance that the agency's objectives will be achieved (a major "Uh oh" will not occur).
3. Measure the system of internal control (ensure that the alarm system is working properly).

For me in looking at these three reasons that I have listed it seems that I have basically stated the same concept in three different ways. If I had to narrow it down to one single statement I would probably pick number 2. That is because if you give reasonable assurance that the agency's objective will be achieved, then you would be saying that you have used agency risk assessment as a tool to determine the capability and you have used it to measure the system of internal control. Bottom line, the reason for an agency to conduct a risk assessment would be to give reasonable assurance that the agency can achieve its objectives.

The main point is that achieving objectives is the fundamental motivation to conducting an Agency Risk Assessment.

Concepts - Why

In theory, if an agency executes an Agency Risk Assessment process in the appropriate manner, then management should be able to give reasonable assurance that the agency's objectives are being achieved and the following could be benefits of doing so:

(SLIDE 41)

(Read **Slide above and below**)

Concepts - Why

- Increases control consciousness by including all levels of employees in the risk assessment process, those participating will better understand and assume responsibility for effective control and risk management. Corrective actions plans may be more accepted and effective because participants "own" the results.

(SLIDE 42)

Concepts - Why

- Improves communication throughout the agency and increases awareness of objectives.
- Assists in managing agency-wide risks more effectively (for larger agencies).
- Improves the effectiveness and efficiency of the agency and thus increases confidence of the public.
- Improves service to the citizens of the State.
- Decreases findings of external auditors or Legislative audit.

(SLIDE 43)

Concepts - Why

- Increases the success of responding to a changing environment in that it can assist management with evaluating the likelihood and impact of major events and developing responses to either prevent those events from occurring or manage their impact on the entity if they do occur.
- Assists management in moving from a “fire fighting” crisis management philosophy to a more systematic process for addressing issues proactively.

(SLIDE 44)

Concepts - Why

- Decreases the potential for fraud and minimizes the risk of waste and abuse.
- Assists in developing a proper oversight process.
- Facilitates the ability to provide reliable and relevant financial data.
- Gives management reasonable assurance that those in the agency are complying with applicable laws and regulations and policies and procedures.

(SLIDE 45)

Above are a few benefits and reasons why to conduct agency risk assessment.

FRAUD



(SLIDE 46)

Ricky is going to discuss the history of Agency Risk Assessment and how it all began. Take note that he will be talking about the State anti-fraud program. So, let me mention this brief thought about how fraud fits into what we are talking about, and that it is this:

Fraud is a negative factor that can affect an agency's capability of achieving objectives. Fraud is so prevalent within the United States throughout the private and public sectors that COSO (we will discuss who COSO is in just a minute) has recognized it as a negative factor that always needs to be considered when determining if an objective can be met. Fraud, or maybe a better word is corruption, can be so wide-spread though-out an agency that it affects more than one objective and can inhibit an agency from achieving its entire mission. That is why fraud is so emphasized when talking about Agency Risk Assessment and a system of internal control.

In conclusion, fraud is a risk that should be considered and assessed within every objective of an Agency's risk assessment.

Segment 1

History

(SLIDE 47)

HISTORY-(Ricky Quattlebaum presenting)

History of Internal Control

- Securities Act of 1933 & Securities Exchange Act of 1934
- 1949 – AICPA Special Report “Internal Control”
 - Safeguarding of Assets
 - Ensuring Accuracy and Reliability of Accounting Data
 - Promotion of Operational Efficiency
 - Adherence to Prescribed Management Practices

(SLIDE 48)

Let's begin with the history of Agency Risk Assessment. In this section, you will briefly be introduced to the acronym COSO and the how the requirement for Agency Risk Assessments came to be in the Arkansas Financial Management Guide. It will also include a brief introduction to the concept of Internal Control; just keep in mind that Risk Assessment is a vital part of internal control as we will discuss in more detail later, but an understanding of risk assessment must begin with understanding internal control.

1930-40's

In the wake of the Great Depression, the Securities and Exchange Commission issued the Securities Act of 1933 and the Securities Exchange Act of 1934, which required new disclosures of all material information relating to issuance of stock and the company issuing the stock, including information about the management team, and audited financial statements of SEC companies by independent auditors.

1949

As corporations became even bigger and more complex, it became impossible to ignore the aspect of business management and their role of providing reliable financial statements. So AICPA published a special report “Internal Control” defining it as a “safeguarding of assets”, the “ensuring of the accuracy and reliability of accounting data”, the “promotion of operational efficiency” and the “adherence to prescribed management practices”.

History -Continued:

- 1977 – Foreign Corrupt Practices Act
 - Internal Controls began to be embraced due to the need to prevent fraud.
- 1985 – National Commission on Fraudulent Financial Reporting (Treadway Commission)
 - COSO was formed to participate in the study.

(SLIDE 49)

Mid 1970's

Over 400 companies were investigated and admitted to making questionable and/or illegal payments in excess of \$300,000,000 to foreign officials, politicians and political parties. Most notable was Lockheed Martin, who bribed foreign officials in West Germany, Italy, Japan, Netherlands and Saudi Arabia, so that those countries would buy their aircraft. Due to occurrences of illegal payments made by US corporations, the U.S. Congress enacted reforms and passed the Foreign Corrupt Practices Act of 1977 which required companies for the first time to implement internal control systems. It was during this time that the concept of internal control started being embraced due to the need to prevent fraud.

(ii) that a system of internal accounting controls is devised

(a) to provide reasonable assurances that transactions are executed in accordance with management's authorization;

(b) to ensure that assets are recorded as necessary to permit preparation of financial statements and to maintain accountability for assets;

(c) to limit access to assets to management's authorization; and

(d) to make certain that recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.”

1985 Introduction of COSO – S&L Failures.

The National Commission on Fraudulent Financial Reporting (also called the Treadway Commission) was an independent private-sector initiative formed in response to the reforms to inspect, analyze and make recommendations on fraudulent corporate financial reporting. The Commission studied the issues from October 1985 to September 1987. James C. Treadway, Jr. was the first chairman of the commission. He was former EVP and General Counsel of Paine Webber and former Commissioner of the Securities and Exchange Commission.

COSO

- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
 - American Institute of CPA
 - American Accounting Association
 - Financial Executive Institute
 - The Institute of Internal Auditors
 - Institute of Management Accountants

(SLIDE 50)

The Committee of Sponsoring Organizations of the Treadway Commission was formed (also known as COSO) to be a part of this Commission and participate in the study.

COSO is made up of five major professional associations:

1. The American Accounting Association (AAA)
2. The American Institute of Certified Public Accountants (AICPA)
3. Financial Executives International (FEI)
4. The Institute of Internal Auditors (IIA)
5. And the Institute of Management Accountants (IMA).

COSO's Objectives

- Establish a common definition of Internal Control
- Provide a standard against which organizations can assess their internal control systems
 - Internal Control-Integrated Framework-1992

(SLIDE 51)

1987

The Treadway Commission issued a report of findings and recommendations in October 1987. In the report, as a part of one of the 49 findings, it was mentioned that entities “should maintain internal controls that provide reasonable assurance that fraudulent financial reporting will be prevented or subject to early detection” and that COSO should develop an integrated framework of internal control.

At this point in time the definition of internal control was not agreed upon by the professional associations. It was important that if entities were to maintain internal control, then there should be a unified description of internal control.

Internal Control Definition

- Internal Control is a *process*, effected by an entity's board of directors, management, and other *personnel*, designed to provide *reasonable assurance* regarding the achievement of *objectives* in the following categories:
 - Effectiveness and efficiency of operations
 - Reliability of Financial Reporting
 - Compliance with applicable laws and regulation

(SLIDE 52)

1992

COSO presented the first report titled “Internal Control—Integrated Framework” in September of 1992. This framework included 5 components of internal control.

Internal control, as defined by COSO, is a process, affected by an entity's board of directors, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the following categories: 1) Effectiveness and efficiency of operations, 2) Reliability of financial reporting, and 3) Compliance with applicable laws and regulations.

This definition is intentionally broad as it is applicable to organizations of varied sizes that operate in different industries and countries. However, it reflects certain fundamental concepts about internal control:

Geared to the achievement of objectives in one or more categories – operational, reporting and compliance.

A process consisting of ongoing tasks and activities – a means to an end, not an end in itself
Effected by people – not merely about policy and procedure manuals, systems and forms, but about people and the actions they take at every level of an organization to affect internal control

Able to provide reasonable assurance – but not absolute assurance, to an entity's senior management and board of directors

Adaptable to the entity structure – flexible in application for the entire entity or for an operating unit or even business process.

Components of Internal Control

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

(SLIDE 53)

There are five components of internal control. These components are control environment, risk assessment, control activities, information and communication, and monitoring activities. These will be discussed in detail in Segment 2.

History - Continued:

- 2000 – Executive Internal Audit Function
- 2002 – SAS99 *Consideration of Fraud in a Financial Statement Audit*
 - *Required external auditors to assess an entity's management anti-fraud program and controls.*

(SLIDE 54)

2000

An executive branch internal audit function was created to promote accountability, integrity and efficiency in the operation of executive branch. In trying to assess internal controls in state government, it became clear at that time that internal control was viewed as segregation of duties and if agencies did not have a proper segregation of duties, legislative audit would tell them. It was clear that a process needed to be put in place to address the integrated framework component of internal control.

2001

Enron—Author Andersen auditors didn't report the fraud.

2002

SAS 99 became effective for audits of financial statements for periods beginning on or after December 15, 2002.

SAS 99: Statement on Auditing Standards #99 *Consideration of Fraud in a Financial Statement Audit* was issued by the Auditing Standards Board of the American Institute of Certified Public Accountants, which detailed auditors responsibilities related to identifying fraud in the audits of financial statements. Among other things it required external auditors to assess an entity's management anti-fraud programs and controls.

History - Continued:

- KPMG – 6/30/03 Audit report listed several material weaknesses.
 - Lack of a Comprehensive Fraud Program
 - Lack of formal, statewide code of conduct
 - Lack of consistency in coordinating ethics and fraud control elements across the state, various features of the existing framework are not cohesively linked...
 - No statewide method to enable anonymous reporting
 - Use of background checks inconsistent

(SLIDE 55)

KPMG (the State's external auditors) reported in the 6/30/03 financial audit that the state lacked a formal ethics and fraud control framework. Repeated finding in the 6/30/04 audit.

History - Continued

- KPMG – 6/30/04 Audit Report (repeat findings)
- 2004 – State Anti-Fraud Measures listed in the Arkansas Financial Management Guide
 - Agency Code of Ethics and Anti-Fraud Policy
 - Background Checks
 - Fraud Reporting Line
 - Fraud Risk Assessment

(SLIDE 56)

The result was a statewide anti-fraud policy that included a formal code of ethics, background checks, fraud hotline and a formal fraud risk assessment, which was geared after the model policy in the appendix to SAS 99.

2004

Effective October 2004, as a part of an initiative to develop the State anti-fraud program, the Department of Finance and Administration (DFA) implemented by way of the Financial Management Guide (R1-19-4-505) a requirement of agency submission of a risk assessment every two years.

This rule included instructions for agencies to submit a risk assessment to the DFA-Office of Accounting, Internal Audit Section. Agency risk assessments are currently due at the end of March of even numbered years.

In the first year of the risk assessment process, agencies were led to just address Fraud and Financial type risks. Subsequent submissions included operational and compliance type risks. Most risk assessments are stronger in the financial objectives and risks, maybe because they are easier to identify or because it is the CFO's or agency financial staff driving the risk assessment process; however, agencies are encouraged to try and expand on operational and compliance objectives and risks.

History - Continued:

- 2013 – Updated COSO Framework
 - Internal Control is a **process**, effected by an entity's board of directors, management, and other **personnel**, designed to provide **reasonable assurance** regarding the achievement of **objectives** relating to operations, **reporting** and compliance.
 - Also included the addition of 17 principles that enhance the framework.

(SLIDE 57)

2013

COSO is still active and updated this framework in March 2013. They updated the definition of internal control by expanding the importance of reporting to non-financial and internal reporting. Current definition:

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

It also included the addition of 17 principles that enhance the framework.

History - Continued:

- COSO Model has become the accepted model.
 - COSO used by Federal Government (OMB Circular A-123 issued in 2004).
 - December 26, 2013 – OMB issued new Omni-Circular titled, *Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards*.

(SLIDE 58)

In the 20 years between the first COSO model roll out and today, the COSO model has become the formal model of Internal Control that everyone follows:

- COSO is used by Federal Government to define Internal Control (OMB Circular A123 issued in 2004). In 2009, when stimulus funds were issued to states, Federal Government wanted to see a risk assessment process in place.

History - Continued:

- OMB Omni-Circular:

*Section 200.393 – Internal Controls – In response to comments that suggested that efforts to mitigate risks of waste, fraud, and abuse would be strengthened by a more explicit reference to existing internal control requirements issued by Government Accounting Office (GAO) and the Committee of Sponsoring Organizations (COSO), the COFAR recommended including this **new section of the guidance which makes explicit non-Federal entity's responsibilities with regard to effective controls.***

(SLIDE 59)

- Dec 26, 2013 OMB issued new Omni-Circular titled, *Uniform Administrative Requirement, Cost Principles and Audit Requirements for Federal Awards. Section 200.393 Internal Controls – In response to comments that suggested that efforts to mitigate risks of waste, fraud, and abuse would be strengthened by a more explicit reference to existing internal control requirements issued by Government Accounting Office (GAO) and the Committee of Sponsoring Organizations (COSO), the COFAR recommended including this new section of the guidance which makes **explicit** non-Federal entity's responsibilities with regard to effective internal controls.*
- COFAR (Council on Financial Assistance Reform)

History - Continued

- AICPA Audit Standards
 - AU-C Section 315 – *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*
 - *Footnote:* This section recognizes the definition of internal control contained in *Internal Control – Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission.

(SLIDE 60)

- Audit Standards issued by the American Institute of Certified Public Accountants

AU-C Section 315 - *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*

Audit procedures to obtain an understanding of the entity and its environment, including the entity's internal control, to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and relevant assertion levels.

¹ This section recognizes the definition and description of *internal control* contained in *Internal Control-Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission.

So that is the timeline and history of how Agency Risk Assessment came to be in the State of Arkansas.

Segment 1

Requirement

(SLIDE 61)

REQUIREMENT

The requirement to submit an Agency Risk Assessment can be found in the Financial Management Guide as rule R1-19-4-505.

Requirement

- Executive Branch State Agencies
- Management
 - Responsible for Achieving Objectives
 - Responsible for overall Internal Control System
 - Remember Definition: Process, personnel, reasonable assurance, achievement of objectives.
 - Sign the Certification Letter
- Managers that are responsible for achieving the specific objectives should be involved

(SLIDE 62)

The requirement for submitting an Agency Risk Assessment is for Executive Branch State Agencies. Constitutional Agencies and Offices are encouraged to submit such, and several do so.

Management is responsible for achieving objectives and; therefore, is responsible for identifying the objectives. Management is also responsible for the overall system of internal control. For this reason management is required to sign a certification letter stating that this is understood and submit that letter with the Agency Risk Assessment document.

Managers that are responsible for achieving specific objectives should be involved in the brainstorming sessions. The brainstorming sessions will be discussed in Segment 2 of this presentation and in the Control Self-Assessment workshop.

Requirement Continued

- **Management's Role**
 - Lead the process by determining objectives
 - Determining and rating risk
 - Determining if controls are sufficient
 - Determining appropriate Corrective Action Plans

(SLIDE 63)

Management should (read slide).

Requirement Continued

- **Risk Assessment Coordinator**
 - Coordinate and Organize the Risk Assessment
 - Facilitate any brainstorming sessions
 - Assist in the documentation process
 - Coordination with DFA-IA (Submission, Communication)

(SLIDE 64)

Back when Agency Risk Assessment was rolled out in 2004-5, we recommended that someone within the agency be designated as the “Risk Assessment Coordinator”. It was intended that this person (read slide). We will discuss more about the Risk Assessment Coordinator in the Control Self-Assessment workshop.

Segment 2

Components of the Agency Risk Assessment

(SLIDE 65)

THE COMPONENTS OF THE AGENCY RISK ASSESSMENT-(Maggie Garrett presenting)

R1-19-4-505

- Two-year cycle
 - Objectives determined by management
 - Brainstorming workshops/sessions
 - All levels of employees
 - Review identified risks and current control activities
 - Discuss if other risks are present
 - Turn in by the end of March of even numbered years
 - Document risks and control activities as they arise
 - Repeat

- Component examples on website

(SLIDE 66)

The requirement for State agencies to submit an Agency Risk Assessment every two years can be found in the Financial Management Guide, R1-19-4-505. If you read the entire section of rule R1-19-4-505 you will not find a great deal of detailed guidance on what exactly needs to be submitted to meet the requirement. In just a minute I will show you where to find more specific information.

First, let's discuss the recommended cycle for completing the risk assessment. Ricky mentioned the Risk Assessment Coordinator. This is an individual within the agency that helps to coordinate the Agency Risk Assessment. The Risk Assessment Coordinator can assist with all steps in the process. The first step is for management to identify the objectives. Again, objectives should be identified with enough detail to ensure that all risks are considered. The Risk Assessment Coordinator can assist with this process and help management ensure that all objectives are covered. We will go over some ways and tips for the Risk Assessment Coordinator to do this in the Control Self-Assessment Workshop. Ultimately, however, it is management's responsibility to identify the objectives.

Once the objectives are identified then brainstorming sessions can be scheduled with all levels of employees to identify risks and control activities. The Risk Assessment Coordinator can assist with scheduling these meetings. We will also talk about these brainstorming sessions in the Control Self-Assessment Workshop. If during the brainstorming sessions participants determine that a corrective action plan should be implemented, then that is recorded during the session. Several ideas for corrective action plans can be documented at this time. Management will determine if a corrective action plan is needed and if so, will also determine the corrective action plan to implement with those documented in mind.

Note, for those corrective action plans that are implemented immediately, those should be documented in the final Agency Risk Assessment document as control activities (in the control activities column of the document). For those corrective action plans that will not be implemented until a future date, due to whatever circumstances, those should be documented in the final Agency Risk Assessment document as corrective action plans and a date for implementation should be included.

This final document will be submitted to DFA-IA at the end of March of even numbered years.

After the document is submitted, and throughout the next two years, management should document any new risks that emerge and the control activities put into place as they occur.

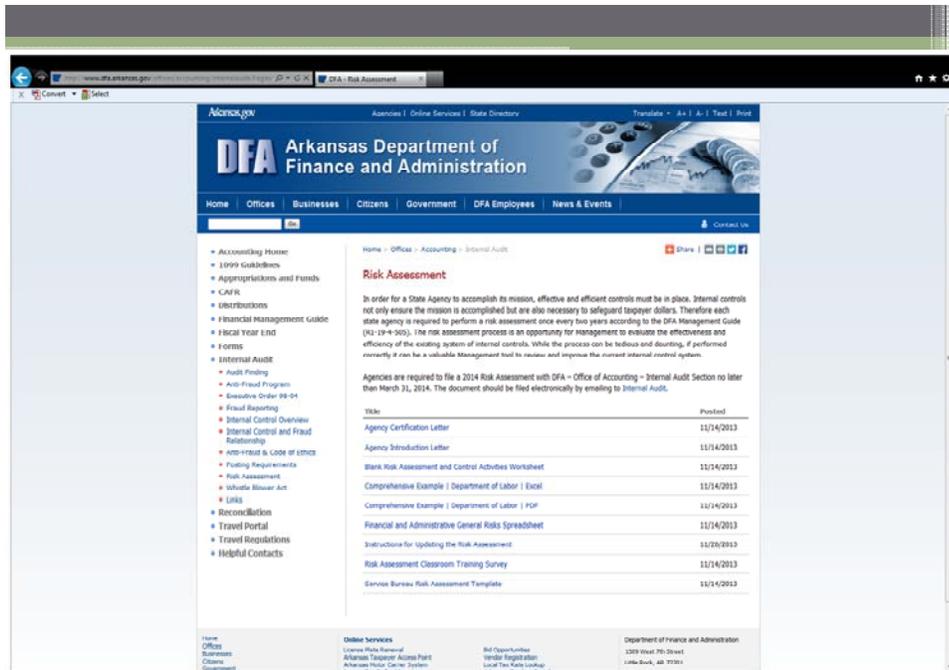
Then, before the Agency Risk Assessment is due again, the brainstorming sessions should be conducted with all levels of employees and all risks and control activities should be discussed, along with any new risks and control activities, to ensure that everyone is aware of the job duties for which they should be performing.

Again, after the brainstorming sessions are done and management reviews and completes the final Agency Risk Assessment document, it is to be submitted to DFA-IA.

This process cycles and repeats every two years.

Now, for the components of the Agency Risk Assessment: we have discussed the concepts surrounding each component already in segment 1, the components are objectives, risks, ratings, control activities, management conclusions, and corrective action plans. We will walk through and discuss in detail the components in the Control Self-Assessment workshop, including tips and tools for identifying each. So, for this segment rather than repeating the same information again, let me show you where to find more detail information about each of the components and some examples that can be utilized in compiling the Agency Risk Assessment, as well as in the brainstorming sessions.

This information can be found on the DFA-IA website.



(SLIDE 67)

<http://www.dfa.arkansas.gov/offices/accounting/internalaudit/Pages/RiskAssessment.aspx>

The web address is:

<http://www.dfa.arkansas.gov/offices/accounting/internalaudit/Pages/RiskAssessment.aspx>

Or the web page can be accessed from the Arkansas.gov webpage (<http://www.arkansas.gov>) by hovering over the word “Government” from the top menu bar and clicking “List of Agencies” and then selecting “Finance and Administration, Arkansas Department of” and then click on the website address for DFA “ www.dfa.arkansas.gov “. Click on “Accounting” on the menu bar on the left-hand side of the screen, and then click on “Internal Audit” from the list on the left-hand side of the screen, then click on “Risk Assessment” on the menu on the left-hand side of the screen.

This will bring you to the page shown in the slide above.

Before we walk through the documents posted on this page, I want to talk about the difference between service bureau and user agencies. To do this, I have a five question quiz.

Q: There are technically around 122 state agencies. Do all of these state agencies have in-house users that have access to enter data into AASIS?

A: No

Q: Approximately, how many state agencies (of the 122) do you think do not have in-house users that can enter data into AASIS?

A: About 76 state agencies do not have in-house users that enter data into AASIS. Although many of these can view the data they cannot enter data.

Q: How are transactions processed from the agencies that do not have in-house users to enter data into AASIS?

A: These agencies send appropriate documentation to the Department of Finance and Administration (DFA).

(SLIDE 68)

Question: There are technically around 118 state agencies. Do all of these state agencies have in-house users that have access to enter data into AASIS? *By entering data I mean entering PO's, receipts, journal entries, etc.*

Answer: No

Question: Approximately, how many state agencies (of the 118) do you think do not have in-house users that can enter data into AASIS? *They may have the ability to view it, but not enter it.*

Answer: About 69 state agencies do not have in-house users that enter data into AASIS. Although many of these can view the data they cannot enter data.

Question: How are transactions processed from the agencies that do not have in-house users to enter data into AASIS?

Answer: These agencies send appropriate documentation to the Department of Finance and Administration (DFA). The office within DFA to which they send the documentation varies and is dependent upon the type of transaction that needs to be processed. For the most part, there are three offices that assist these agencies. They are Office of Personnel Management, Office of State Procurement, and Office of Accounting-Service Bureau Section.

Q: What does the term “Service Bureau Agency” mean?

A: It is a distinction between Arkansas state agencies that means the agency does not have in-house user access to enter data into AASIS.

Q: Why are there service bureau agencies?

A: A service bureau agency usually has a small number of employees and to assist with continuity of data entry into AASIS, DFA processes the transactions for these agencies.

- Service Bureau Agency is an agency that does not have in-house user access to enter information into AASIS
- User Agency has an in-house employee that processes transactions directly into AASIS.

(SLIDE 69)

Question: What does the term “Service Bureau Agency” mean?

Answer: It is a distinction between Arkansas state agencies that means the agency does not have in-house user access to enter data into AASIS.

Last Question: Why are there service bureau agencies?

Answer: A service bureau agency usually has a small number of employees and to assist with continuity of data entry into AASIS, DFA processes the transactions for these agencies.

Service Bureau Agency is an agency that does not have in-house user access to enter information into AASIS and a User Agency has an in-house employee that processes transactions directly into AASIS.

The reason that this is important for the purpose of Agency Risk Assessment is because, Service Bureau Agencies can have different risks and controls than user agencies because of this distinction (smaller number of employees and different process for entering transactions); and, this is important to know because on the website there is certain information for service bureau agencies and certain information for user agencies. So keep that in mind.

(GO TO INTERNET)

Agency Certification Letter

- **Purpose**
This document is to be submitted with the Agency Risk Assessment on the agency's letterhead. It states that management is responsible for establishing and maintaining an effective system of internal controls. Only one letter per agency is required.
- **The three paragraphs**
There are three paragraphs and the one that relates to the results of the risk assessment is the one that should be shown on the letter with the other two being deleted.

The first paragraph is for an Agency risk Assessment that has all sufficient controls in place. This is the designation in the management conclusion column on the Agency Risk Assessment document. If the management conclusions for all risks are "S" (for "Sufficient") then this paragraph should be selected.

The second paragraph is for the Agency Risk Assessment, which has the results of some "NS" (for "Not Sufficient") determinations but all of those determined to be not sufficient have corrective action plans.

The third paragraph is for the Agency Risk Assessment, which has the results of some "NS" determinations but for one or more of those "NS" conclusions a corrective action plan could not be implemented.

- **About the signatures**
There are three blanks on this document for signatures. Only two signatures are required. It is preferred that the Agency Director and CFO sign the letter; however, for small agencies where one or more of these positions do not exist then it is acceptable for the individual completing the Agency Risk Assessment sign along with an Officer of the Board or Commission.

Agency Introduction letter

- **Purpose**
This letter was sent in November of 2013 and was to give notice that the Agency Risk Assessment was due in March for 2014.

Blank Risk Assessment and Control Activities Worksheet

- Purpose
This document has instructions for each field of the Agency Risk Assessment form and a blank form. This is an Excel workbook and there are two tabs which can be accessed at the bottom of the screen.

Instructions tab

Most of the instructions for each field are self explanatory except for the “Objective Type”. This field can be used by the agency to ensure that all types of objectives are considered within the Agency Risk Assessment. The types of objectives defined by COSO are reporting, operational and compliance. If management uses this field then each objective would be analyzed to determine which category each objective falls within (one objective can be categorized within more than one type). After this analysis, management can easily ensure that all objective types have been considered. There should be at least one of each objective type with the Agency Risk Assessment as a whole.

The types that are listed are:

F=Financial Objective (COSO has changed the internal control definition from focusing on financial reporting to focusing on all reporting of an entity. So, this objective type is now considered a “Reporting” objective.)

O=Operational Objective (no change)

C=Compliance Objective (no change)

Fr=Fraud Objective (this was an objective type that was used when the Agency Risk Assessment was first rolled out in 2004-5 to assist in ensuring that fraud was considered with the Agency Risk Assessment. This presentation; however, used a different method for fraud consideration which was to consider fraud as a risk within each objective. Both methods for considering fraud are acceptable. The point is that fraud is considered in the Agency Risk Assessment.)

The other notable fields are:

Significance/Impact rating: Large, Moderate, or Small

Likelihood rating: High, Medium, Low

Management Conclusion: “S” for sufficient and “NS” for not sufficient.

Blank Risk Assessment tab

This is the form that is used to submit the Agency Risk Assessment document.

Comprehensive Example/Department of Labor

- Purpose
This is an example of an USER Agency Risk Assessment. Note the organization of the departments and activities.
- There are two file formats, Excel and PDF

Financial and Administrative General Risks Spreadsheet

- Purpose
This Excel workbook has examples and suggestions of risks and control activities for USER agencies. There are several activities presented, each is listed on a separate tab which are titled at the bottom within the workbook.
- This is not an all inclusive list and while the control activities lists are considered sufficient, they are not necessarily what are required to be in place at the agency. Management should ensure that the control activities listed within the Agency Risk Assessment are those that are actually performed.
- Agency position titles should be used. If there is more than one position that share the same name, then a number designation can be used. For example, Administrative Assistant 1, Administrative Assistant 2, etc.

Instructions for updating the risk assessment

- Purpose
This gives very brief step by step instructions on how to fill out the risk assessment.

Notable information:

Step One:

This step mentions reviewing a copy of the letter sent from DFA-IA. These letters were issued to agency management for Agency Risk Assessments that were reviewed by our office. Not all Agency Risk Assessments were reviewed.

Step Nine:

This step discusses the certification letter that is to be submitted by agency management to DFA-IA and gives instructions on who should sign the letter and where the letter should be mailed. The signatures were discussed earlier.

Also, it is acceptable to scan the original certification letter and email DFA-IA the scanned version along with the submission of the Agency Risk Assessment. If the scanned version is sent through email the mailed version is not needed.

Step Ten:

This step mentions that the final Agency Risk Assessment document should be submitted in the Excel version to InternalAuditAcc@dfa.arkansas.gov.

Service Bureau Risk Assessment Template

- Purpose
This Excel workbook has examples and suggestions of risks and control activities for SERVICE BUREAU agencies. There are several activities presented, each is listed on a separate tab which are titled at the bottom within the workbook.
- It has been updated since the last cycle.
- The instructions tab has been updated. It mentions that there are assumptions for this template: it has 3 employees, it is a regulatory board or commission, and utilizes a commercial bank account and the Arkansas State Treasury. Delete what is not relevant and add anything that is; for example, if the agency does not use a commercial bank account, then anything mentioned about a commercial bank account in the template should be deleted. If the agency has 5 employees instead of 3, then changes to the control activities would need to reflect such. If the agency has an objective that is not listed then that should be added along with the risks and control activities that relate. So forth and so on.
- This can be a starting point:
 - Add/Delete objectives, risks and control activities as appropriate.
 - Fill in the significance/impact and likelihood ratings (per risk)
 - Ensure the control activities reflect those that the agency actually has in place. Use the agency position names. If a there is more than one position that share the same name, then a number designation can be used. For example, Administrative Assistant 1, Administrative Assistant 2, etc.
 - Fill in the management conclusions, for each risk and at the bottom. Note, DFA-IA considers the controls as listed in this document as sufficient so if the agency does perform the control as stated then the management conclusion can be “S”.

Segment 2

How Agency Risk Assessment Relates
to the System of Internal Control

(SLIDE 71)

HOW AGENCY RISK ASSESSMENT RELATES TO THE SYSTEM OF INTERNAL CONTROL

To determine how agency risk assessment relates to the system of internal control for an agency, first you need to know what agency risk assessment is (which is what we've been talking about up to this point but as a reminder):

Risk Assessment ↔ Internal Control

Agency Risk Assessment is a process used by management of an agency to identify, analyze and manage the potential risks that could hinder or prevent the agency from achieving its objectives.

- Can be used as a tool to measure internal control
- Is a part of the system of internal control

(SLIDE 72)

Agency Risk Assessment is a process used by management of an agency to identify, analyze and manage the potential risks that could hinder or prevent the agency from achieving its objectives.

- We mentioned that the agency risk assessment can be used as a tool to measure internal control.
- We also talked earlier about how agency risk assessment is a part of the system of internal control.

Agency risk assessment relates to internal control in these two ways and the remainder of the discussion for this segment I will expand on what these mean. To do this we need to talk about what a system of internal control is.

Risk Assessment ↔ Internal Control

- COSO framework state that “Internal Control” is a process that has five interrelated components:
 - Control Environment
 - Risk Assessment
 - Control Activities
 - Information and Communication
 - Monitoring

“present”, “functioning”, and “operating together”.

(SLIDE 73)

- I have already mentioned that internal control is like an alarm system that can give notice about the capability of achieving an objective. This was mentioned toward the end of Segment 1 of this presentation. What you will find as you learn about that which is comprised within internal control is that if the five components are present, functioning and operating together, then management will be alerted, in a timely manner, when significant risks emerge.
- Ricky talked about COSO’s definition of internal control and about how it was defined by COSO, as a process, affected by an entity’s board of directors, management and other personnel designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
 - 1) operations, 2) reporting, and 3) compliance.
- He also mentioned that the COSO framework states that “Internal Control” is a process that has five interrelated components:
 1. Control Environment
 2. Risk Assessment
 3. Control Activities
 4. Information and Communication
 5. Monitoring

For an agency to have effective internal control means that they have these five components appropriately integrated within the agency; COSO says that each should be “present”, “functioning”, and “operating together”.

Agency risk assessment can be used as a tool to measure internal control.

I said before I'm going to expand on how agency risk assessment can be used as a tool to measure internal control. Understand that a system of internal control is measured in strength. So, the strength of a system is determined by the number and severity of weaknesses. Thus, the word "weakness" is used when describing this measurement.

Risk Assessment ↔ Internal Control

- “Present” and “Functioning”
 - Although the agency risk assessment document does not prove that the components are actually “present” and “functioning” within the agency, it does set the standard for what management expects to be present and functioning.
 - If management does not expect a strong system of internal control, then the actual system of internal control will not be strong

(SLIDE 74)

The five components should be present and functioning (according to COSO). Although the Agency Risk Assessment document doesn't prove that the components are actually “present” and “functioning” within the agency, it does set the standard for what management expects to be present and functioning.

There is a direct relationship between management's expectation of internal control and the strength (or weakness) of the actual system of internal control. In other words, if management does not expect a strong system of internal control, then the actual system of internal control will not be strong; the agency risk assessment document is a testament of what the internal control system is expected to be.

Risk Assessment ↔ Internal Control

- “Operating together”
 - The concept of “operating together”, of components being interrelated, intermingled, interconnected is why the document that is submitted by agencies gives evidence the five components of internal control and thus a tool to use to measure internal control.

(SLIDE 75)

The concept of “operating together”; of components being interrelated, intermingled, interconnected is why the document that is submitted by agencies gives evidence of the five of the components of internal control and thus a tool to use to measure internal control. I will give some examples of this in a minute.

Component Definition & Principles

1. What should be in an internal control system
2. Hypothetical situations of weaknesses
 - Not an all inclusive example
3. How the agency risk assessment relates to the component and gives evidence of weaknesses within the system of internal control

(SLIDE 76)

Component Definition and Component Principles

In discussing the five components, we are going to look at each individual component and discuss what they are. We will read through the definitions that COSO has set for each component and then read through the principals (remember Ricky mentioned earlier that there are 17 principles of internal control) for each component. This is what should be in an internal control system.

Then we are going to look at hypothetical situations of weaknesses of internal control that would be categorized in each component. I have only listed a few per component so realize it's not an all inclusive or limited to only the situations that I present today.

Finally, the third thing that we will look at with each component is how the agency risk assessment relates to the component and gives evidence of weaknesses within the system of internal control.

Component Definition & Principles

****If you are reviewing the agency risk assessment and you see the following issues, then realize that it could mean that your agency has an internal control weakness or it could mean that what is written is not representative of the agency's intent and should be properly updated.****

(SLIDE 77)

Also, the examples that I will present relating to an agency's risk assessment were not pulled from any agency risk assessment; I made them up. If you think that your agency's risk assessment has something similar to what I present appearing in it, then it would be best to ensure that the information is stated so that it is truly representative of the agency's perspective. Know that I understand that in some cases those who put together the agency risk assessments are not fully trained and may not understand the concepts of agency risk assessment, or maybe those who compiled the risk assessment do not have strong skills in written communication. However, if you are reviewing the agency risk assessment and you see these issues that I am about to list, then realize that it could mean that your agency has an internal control weakness or it could mean that what is written is not representative of the agency's intent and should be properly updated.

Regardless, I am not pointing out or pointing to any one risk assessment specifically, they are just examples to emphasize the concept of how internal control relates to the agency risk assessment.

Control Environment-Definition

- *Set of standards, processes, and structures*
- *Tone at the top*
- *Management reinforces expectations at the various levels of the organization*
- *Integrity and ethical values*
- *Parameters enabling the board of directors to carry out its governance oversight responsibilities*
- *The organizational structure and assignment of authority and responsibility*
- *The process for attracting, developing, and retaining competent individuals*
- *The rigor around performance measures, incentives, and rewards to drive accountability for performance*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 78)

Beginning with the first component of internal control, which is “Control Environment”.

Control Environment: Component Definition

“The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control including the expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.”

Source: COSO Internal Control-Integrated Framework March 2013.

Control Environment-Principles

- 1. The organization demonstrates a commitment to integrity and ethical values.*
- 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*

(SLIDE 79)

Control Environment: Component Principles

- 1. The organization demonstrates a commitment to integrity and ethical values.*
- 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.*

Control Environment-Principles

3. *Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*
4. *The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*
4. *The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 80)

3. *Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.*
4. *The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.*
5. *The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.*

Source: COSO Internal Control-Integrated Framework March 2013.

Tone at the top is a phrase used commonly with this component and this phrase still applies, but the definition and principles also include the organizational structure; it points to look at the authority that is given to individuals and additionally to consider how individuals are held accountable. These are things that are included in a system of internal control that are categorized in this component.

Control Environment

Example Weaknesses

- If an employee of a state agency were reviewing and rating other employees on performance evaluations where the rating employee did not supervise those being rated.
- If supervisors have positions to fill where the job specifications used to advertise and select applicants did not match the actual job duty or the job needs; that would be considered a weakness in internal control.

(SLIDE 81)

Here are some examples of weaknesses that might be categorized within this component:

- a. If an employee of a state agency were reviewing and rating other employees on performance evaluations where the rating employee did not supervise those being rated.
- b. If supervisors have positions to fill where the job specifications used to advertise and select applicants did not match the actual job duty or the job needs; that would be considered a weakness in internal control.

Control Environment

Example Weaknesses

- If management displayed that inappropriate actions were acceptable, then that would be considered a weakness in internal control.
- If management set reporting of important matters at a level where they would not be aware of those issues (so that they can claim that they didn't know— “plausible deniability”) then that would be considered a weakness in internal control.

(SLIDE 82)

- c. If management displayed that inappropriate actions were acceptable, then that would be considered a weakness in internal control.
- d. If management set reporting of important matters at a level where they would not be aware of those issues (so that they can claim that they didn't know— “plausible deniability”) then that would be considered a weakness in internal control.

Control Environment

Example Weaknesses

- If the agency doesn't have an official code of conduct.
- If individuals are not held accountable for their internal control responsibilities.

(SLIDE 83)

- e. If the agency doesn't have an official code of conduct.
- f. If individuals are not held accountable for their internal control responsibilities.

Control Environment

Example weaknesses that might be evident in an agency risk assessment

RISK:

Performance evaluations are not completed accurately or timely

CONTROL ACTIVITY:

Our agency has 100 employees who are rated by the CFO of the agency.

(SLIDE 84)

Here are some examples of how a weakness categorized within this component of internal control might be evident in an agency risk assessment.

- An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Performance evaluations are not completed accurately or timely

CONTROL ACTIVITY:

Our agency has 100 employees who are rated by the CFO of the agency.

Why would this indicate an internal control weakness? Because it would be hard to believe that one person, the CFO, would have direct authority over 100 employees in that the CFO would know the daily work and activities of each employee. That in itself is not feasible. Here we have the situation that I just described in the first weakness mentioned--If an employee of a state agency were reviewing and rating other employees on performance evaluations where the rating employee did not supervise those being rated.—so this could indicate that a weakness in internal control exists.

Control Environment

Example weaknesses continued

RISK:

Employees share passwords

CONTROL ACTIVITY:

Our employees have to share passwords to perform their job duties.

(SLIDE 85)

An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Employees share passwords

CONTROL ACTIVITY:

Our employees have to share passwords to perform their job duties.

Why would this indicate that the control environment component of internal control had a weakness for this agency? Because having user ids and passwords for any computer system is a control activity itself. There are several purposes for using this type of control activity, one of which is to limit the abilities of users in the computer system. So by sharing passwords these control activities are circumvented. If management accepts that circumventing controls is okay, then that would speak to the control environment. Circumventing controls would be a weakness in the system of internal control.

Risk Assessment-Definition

- *Risks from external and internal sources*
- *Involves identifying and assessing risks*
- *Forms the basis for determining how risks will be managed*
- *A precondition to risk assessment is the establishment of objectives*
- *Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives*
- *Requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.”*

Source: COSO Internal Control-Integrated Framework March 2013

(SLIDE 86)

Risk Assessment: Component Definition

“Every entity faces a variety of risks from external and internal sources. Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.

A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyze risks to those objectives. Management also considers the suitability of the objectives for the entity. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.”

Source: COSO Internal Control-Integrated Framework March 2013.

Risk Assessment-Principles

6. *The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*
7. *The organization identifies risks to the achievement of its objectives across the entity and analyzes the risks as a basis for determining how the risks should be managed.*

(SLIDE 87)

Risk Assessment: Component Principles

6. *The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*
7. *The organization identifies risks to the achievement of its objectives across the entity and analyzes the risks as a basis for determining how the risks should be managed.*

Risk Assessment-Principles

- 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.*
- 9. The organization identifies and assesses changes that could significantly impact the system of internal control.*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 88)

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

A risk assessment process must be in place for this component to be evident.

Risk Assessment

Example Weaknesses

- If objectives are not specified clearly to enable the identification of risks.
- If significant risks not are identified.
- If the potential for fraud is not addressed in risk identification.
- If there is no process in place to communicate risks.
- If the ratings for the risks are assessed inappropriately.

(SLIDE 89)

Here are some examples of weaknesses that might be categorized within this component:

- a. If objectives are not specified clearly to enable the identification of risks.
- b. If significant risks not are identified.
- c. If the potential for fraud is not addressed in risk identification.
- d. If there is no process in place to communicate risks.
- e. If the ratings for the risks are assessed inappropriately. An employee may not think a risk is that big of a deal, but their manager may think that the risk is a big deal because the manager may know how it might affect the agency from a different perspective.

Risk Assessment

An agency may have a weakness in internal control if an agency risk assessment:

- is never submitted
- is missing major departments and/or activities of the agency
- has only one risk per objective
- rated the likelihood and significant ratings all the same for every risk

(SLIDE 90)

Here are some examples of how a weakness categorized within this component of internal control might be evident within an agency risk assessment.

- An agency may have a weakness in internal control if an agency risk assessment is never submitted.

Why would it be an internal control weakness if an agency never submitted an agency risk assessment? Because the process for identifying and analyzing the agency's system of internal control has likely not been done. If there is not process for such identification and analysis, then that is considered an internal control weakness.

- An agency may have a weakness in internal control if the agency risk assessment is missing major departments and/or activities of the agency.

Why would it be an internal control weakness if an agency's risk assessment is missing major departments and/or activities of the agency? Same reason as the last weakness we discussed, the process for identifying and analyzing the agency's system of internal control has likely not been done for those objectives for which the missing departments and/or activities represent. If there is not a process for such identification and analysis, then that is considered an internal control weakness even if it is for part of the agency. Completeness is important when compiling the agency risk assessment.

- An agency may have a weakness in internal control if the agency risk assessment has only one risk per objective.

Why would it be an internal control weakness if an agency's risk assessment has only one risk per objective? This is touching on completeness of the agency risk assessment. There is one of two reasons that an objective has only one risk: 1) all risks were not identified for the objective, or 2) the objectives are too narrowly formed. The weakness is that all risks are not identified and therefore not assessed and managed. Reason #1 would be an obvious issue. For reason #2, if objectives are formed too narrow then there is still a good chance that not all risks were identified.

- An agency may have a weakness in internal control if the agency risk assessment rated the likelihood and significant ratings all the same for every risk.

Why would it be an internal control weakness if an agency's risk assessment had every risk rated the same? If every risk has identical ratings for all the objectives, then that indicates that the ratings were not assessed properly. As we will discuss in the Control Self-Assessment workshop, ratings are to be used by management to allocate resources as necessary. Thus, in theory, resources could be allocated inappropriately if management relied on the stated ratings.

Control Activities-Definition

- *actions established through policies and procedures*
- *ensure that management's directives to mitigate risks to the achievement of objectives are carried out*
- *performed at all levels of the entity, at various stages within business processes, and over the technology environment*
- *may be preventive or detective in nature*
- *may encompass a range of manual and automated activities*
- *Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities."*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 91)

Control Activities: Component Definition

“Control activities are the actions established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, management selects and develops alternative control activities.”

Source: COSO Internal Control-Integrated Framework March 2013.

Control Activities-Principles

- 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*
- 11. The organization selects and develops general control activities over technology to support the achievement of objectives.*

(SLIDE 92)

Control Activities: Component Principles

- 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.*
- 11. The organization selects and develops general control activities over technology to support the achievement of objectives.*

Control Activities-Principles

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Source: COSO Internal Control-Integrated Framework March 2013

(SLIDE 93)

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.”

Source: COSO Internal Control-Integrated Framework March 2013.

Many think of segregation of duties when discussing Internal Control. But, segregation of duties is just a part of what we are calling Internal Control. Internal Control is much bigger than just identifying processes where segregation of duties exists. Segregation of duties is a part of internal control, but would fall under the category of Control Activities. Realize that when we talk about Internal Control, it's the big picture.

So, for this component to be in place, an agency would need to show that there were policies and/or procedures in place to mitigate the risks that had been identified.

Control Activities

Example Weaknesses

- Missing or insufficient control activities
- If control activities are not designed well and hinder the efficiency of the agency.
- If the cost of a control activity out ways the benefit of that which it is trying to protect.
- If written policies do not exist to establish what is expected.

(SLIDE 94)

Here are some examples of weaknesses that might be categorized within this component:

- a. If control activities are not present, but should be, for certain risks; or control activities in place do not mitigate the risk.
- b. If control activities are not designed well and hinder the efficiency of the agency.
- c. If the cost of a control activity out ways the benefit of that which it is trying to protect.
- d. If written policies do not exist to establish what is expected.

Here are some examples of how a weakness categorized within this component of internal control might be evident within an agency risk assessment.

Control Activities

Examples of how a weakness might be evident within an Agency Risk Assessment

RISK:

Lack of Funds

CONTROL ACTIVITY:

[left blank]

(SLIDE 95)

An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Lack of funds

CONTROL ACTIVITY:

[left blank]

Why would it be an internal control weakness if an agency's risk assessment was missing a control activity for a risk? Because control activities are supposed to be in place to ensure that the agency's objectives are achieved. If there is no control, then it is possible that the agency's objective may not be achieved.

Control Activities

Examples continued

RISK:

Employee Theft or Fraud

CONTROL ACTIVITY:

We trust our employees and this will not happen.

(SLIDE 96)

RISK:

Employee Theft or Fraud

CONTROL ACTIVITY:

We trust our employees and this will not happen.

Why would it be an internal control weakness if an agency's risk assessment said this? Because trust is not a control and so, in essence, there is no control for this risk. If there is no control, then it is possible that the agency's objective may not be achieved.

Information and Communication-Definition

- *Management obtains or generates and uses*
- *internal and external sources*
- *enables personnel to receive a clear message*
- *control responsibilities must be taken seriously.*

(SLIDE 97)

Source: COSO Internal Control-Integrated Framework March 2013.

Information and Communication: Component Definition

“Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information, and it provides information to external parties in response to requirements and expectations.”

Source: COSO Internal Control-Integrated Framework March 2013.

Information and Communication-Principles

- 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.*
- 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.*

(SLIDE 98)

Information and Communication: Component Principles

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Information and Communication-Principles

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 99)

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.”

Source: COSO Internal Control-Integrated Framework March 2013.

Within every agency there is information and communication. The strength of this component can be measured by how well the information is obtained, generated, used and communicated (internally and externally); this also includes consideration of the timeliness and accuracy of the information.

Information and Communication

Examples of Weaknesses

- If inaccurate or irrelevant information is used
- If objectives and responsibilities for internal control are not communicated.

(SLIDE 100)

Here are some examples of weaknesses that might be categorized within this component:

- a. If inaccurate or irrelevant information is used.
- b. If objectives and responsibilities for internal control are not communicated.

Information and Communication

Examples of how a weakness might be evident within an Agency Risk Assessment

RISK:

Inaccurate financial information is given to the board.

CONTROL ACTIVITY:

The CFO compiles and reviews the information

(SLIDE 101)

Here are some examples of how a weakness categorized within this component of internal control might be evident within an agency risk assessment.

An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Inaccurate financial information is given to the board.

CONTROL ACTIVITY:

The CFO compiles and reviews the information.

What is wrong with the CFO compiling and reviewing financial information that is given to a board or commission? Nothing, the CFO can compile and review the information. The problem with this control is that which is missing. This control should have someone performing a second review of the information as well. Maybe, for example, the Director should perform a second review. Not necessarily of every single detail, but at least an overall review.

If the Director is not interested in what information is presented to the board, then that would be a sign that there is a weakness in internal control.

Information and Communication

Examples continued

RISK:

Employees are paid for inaccurate number of hours.

CONTROL ACTIVITY:

The agency tracks all timesheets and leave requests.

(SLIDE 102)

An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Employees are paid for inaccurate number of hours.

CONTROL ACTIVITY:

The agency tracks all timesheets and leave requests.

Assume that this is only a part of the control activity and the control activity is complete, what is the issue with this sentence in relation to communication part of this component?

The agency risk assessment process is a good tool to use when defining the control activities to assign who is responsible for doing them. Once assigned then management would be responsible for discussing with the employee what they are to do and the importance of the job duty because it is to be utilized as a control activity. That is why we encourage position titles be used within the control activities of the agency risk assessment document. So for this example, who is responsible for tracking time sheets and leave requests? Who knows? If management doesn't know, then how will the employee know? Part of ensuring that there is an effective system of internal control is for employees to know what their responsibilities are in performing those controls.

Monitoring Activities-Definition

- *Ongoing evaluations, separate evaluations, or some combination of the two are used*
- *built into business processes at different levels of the entity, provide timely information*
- *Findings are evaluated*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 103)

Monitoring Activities: Component Definition

“Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by regulators, recognized standard-setting bodies or management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.”

Source: COSO Internal Control-Integrated Framework March 2013.

Monitoring Activities-Principles

- 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.*
- 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.*

Source: COSO Internal Control-Integrated Framework March 2013.

(SLIDE 104)

Monitoring Activities: Component Principles

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: COSO Internal Control-Integrated Framework March 2013.

There is a common misconception that auditors are responsible for this component. But who is responsible for the system of internal control? Management is. Management is responsible for ensuring that the system of internal control is present and functioning. Now, management can ask that auditors perform the separate evaluations that are discussed in the definition, but ultimately it is still management's responsibility to make sure that is done. Separate evaluations are not the only way to monitor. Management can also build in evaluations into the business processes as well.

Monitoring Activities

Examples of weaknesses

- If monitoring activities do not occur.
- If the reporting of the monitoring activities is biased.
- If the reporting of the monitoring activities goes to those that do not have authority to take corrective action.
- If the reporting of the monitoring activities is not timely.

(SLIDE 105)

Examples of weaknesses in this component are:

- a. If monitoring activities do not occur.
- b. If the reporting of the monitoring activities is biased.
- c. If the reporting of the monitoring activities goes to those that do not have authority to take corrective action.
- d. If the reporting of the monitoring activities is not timely.

Monitoring Activities

Examples of how a weakness might be evident within an Agency Risk Assessment

RISK:

Deposits are not receipted timely.

CONTROL ACTIVITIES:

The Executive Director requests and reviews a list of deposits and the date deposited at year-end.

(SLIDE 106)

Here are some examples of how a weakness categorized within this component of internal control might be evident within an agency risk assessment.

An agency may have a weakness in internal control if the agency risk assessment says:

RISK:

Deposits are not receipted timely.

CONTROL ACTIVITY:

The Executive Director requests and reviews a list of deposits and the date deposited at year-end.

Is the monitoring of when the deposits are receipted appropriate?

Monitoring Activities

An agency may have a weakness in internal control if the agency risk assessment does not mention monitoring of controls within the control activities.

(SLIDE 107)

An agency may have a weakness in internal control if the agency risk assessment does not mention monitoring of controls within the control activities.

If the risk assessment doesn't mention the monitoring of controls then it might be assumed that they are not monitored.

Internal Control

Control Environment Component	By setting the tone at the top
Risk assessment component	By formally identifying and assessing the risks to certain objectives
Control Activities component	By formally identifying and assessing control activities to mitigate the risks
Information and Communication component	By communicating controls to those who will be performing them
Monitoring component	By identifying monitoring activities

(SLIDE 108)

Agency risk assessment is a part of the system of internal control.

The second concept that I wanted to expand upon is that agency risk assessment is a part of the system of internal control, so let's talk about that for a second.

As you can see, one of the components is termed "Risk Assessment". This is not exactly the same thing as our "Agency Risk Assessment". The term used in the COSO definition for Risk Assessment focuses solely on the identification of risks, whereas, the Agency Risk Assessment requires identification of risks, but it goes a few steps further and requires the analysis and management of those risks to be considered and documented as well. So don't be confused by the COSO component which is termed "Risk Assessment" and our term that we use "Agency Risk Assessment".

So, by appropriately conducting an agency risk assessment performance of the components of internal control would be as follows: (Read slide)

In this way, the agency risk assessment is a part of the system of internal control. It's not the whole system, but it can be a supportive part of it.

Goal is to answer the following:

1. What is a risk assessment?
2. Why should risk assessment be done?
3. Who should implement risk assessment?
4. How is risk assessment implemented and documented?
5. What are the components of risk assessment?
6. What happens after risk assessment is complete?
7. What is the future of risk assessment for Arkansas agencies?

(SLIDE 109)

Answer Goal Questions

1. What is risk assessment?

Depends on if you are referring to the Agency risk assessment or the COSO definition of risk assessment. The two are different in that the COSO definition limits risk assessment to just the identification of risks, but the Agency risk assessment term encompasses identification, analysis and management of risks. For the purposes of the term risk assessment as seen on this slide assume that we are talking about Agency Risk Assessment.

2. Why should risk assessment be done?

For management to have reasonable assurance that objectives will be met.

3. Who should implement risk assessment?

Management.

4. How is risk assessment implemented and documented?

Management should determine the objectives, then brainstorming workshops with employees whose job it is to achieve those objectives should be conducted to brainstorm risks and determine current control activities. The brainstorming workshops should begin the documentation process where a recorder is recording the information, management should review the results of the brainstorming workshop if not involved and determine if

and what corrective action plans should be implemented and then the employees responsible for performing control activities should be made aware of any changes in job duties due to corrective action plans.

5. What are the components of risk assessment?

The main components of Agency risk assessment are:
Objectives, risks, risk ratings, control activities, management conclusions, and corrective action plans.

6. What happens after risk assessment is complete?

After management has determined the corrective action plans needed, if needed, then the agency risk assessment document is sent to our office every two years.

7. What is the future of risk assessment for Arkansas agencies?

It is our hope that agencies will utilize the Agency Risk Assessment process to better the efficiency and effectiveness of the agency.