

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

Function: Agency Risk Assessment: Control Self-Assessment Workshop  
Location: Highway and Transportation Conference Room  
Date: February 2014  
Time: 1:30-3:30

Preface

The following narrative is that which corresponds to the PowerPoint Slide show that was presented at the Control Self-Assessment Workshop February 20, 2014. Several Control Self-Assessment 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 was to provide a “teaching the teachers” workshop, where those who coordinate and/or implement an agency risk assessment would learn the “control self-assessment” approach. The workshop provided guidance on 1) how to organize the risk assessment so that all material objectives would be documented, 2) tools to lead management and line-level employees in brainstorming sessions to ensure that all major risks would be considered, and 3) tips to ensure that sufficient controls would be included. The training was not agency-specific, but rather provided general tools, techniques, and methodology for completing an Agency Risk Assessment. This workshop was for those who already had a basic knowledge of risk assessment and desired to improve the efficiency and effectiveness of the risk assessment process.

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 By: \_\_\_\_\_  
 Activity: \_\_\_\_\_ Date Prepared: \_\_\_\_\_

Objective Type	Objective	Risk Assessment			Address to Manage Risks		Agent Evaluation	Corrective Action Plan	
		Risks	Significant?	Urgent?	Control Activities	Responsible Party		Due 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 objective(s).

2. The control activities are sufficient to mitigate all of the identified risks and provide a reasonable basis for achieving the stated objective(s), except for the control activities that are not sufficient to mitigate the identified risks. The risk or objective control activities needed to mitigate the identified risks is or are included in the Corrective Action Plan (CAP) along with an implementation date. The implementation date is 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 objective(s). Management has not identified any control activities that would be more effective to implement in order to mitigate the risk to an acceptable level. Therefore, we accept the risk that the stated objective(s) may not be achieved.

## Table of Contents

<b>Content Area</b>	<b>Page</b>
<u>Introduction</u>	
Welcome and Contact Information	3
Presentation Structure and Goal Questions	4
<u>Segment 1--Agency Risk Assessment Implementation</u>	6
Control Self Assessment	7
Workshops	11
Objectives	17
Examples	46
Summary	50
<u>Segment 2—Risks and Control Activities</u>	52
Risks	52
Brainstorming Sessions	58
Tool--DFA Office of Accounting Internal Audit Website	60
Tool--List of General Risks	61
Tool--AGA Fraud Prevention Toolkit	64
Examples	81
Ratings	89
Summary	100
Control Activities	101
AGA Fraud Prevention Toolkit	111
Examples	121
Tips	127
Management Conclusions	130
Corrective Action Plans	136
Summary	137
Disaster Recovery Plans	138
Workshop Recap	147

# Control Self-Assessment

2014 Risk Assessment Training

DFA - Accounting - Internal Audit

(Slide 1)

## Introduction

- Welcome to the 2014 Control Self Assessment Workshop
  
- Contact emails:
  - [InternalAuditACC@dfa.arkansas.gov](mailto:InternalAuditACC@dfa.arkansas.gov)
  - [Maggie.Garrett@dfa.arkansas.gov](mailto:Maggie.Garrett@dfa.arkansas.gov)

(Slide 2)

## Segment 1

- Agency Risk Assessment Implementation
- Objectives



(Slide 3)

## Segment 2

- Risks
- Control Activities



(Slide 4)



## Goal is to answer the following:

1. What is the Control Self-Assessment approach to risk assessment?
2. What is the role of the risk assessment coordinator?
3. What is an effective and efficient way for an organization to conduct risk assessment?
4. How should risk assessment be documented and organized?
5. What are objectives and how should they be formed?

(Slide 5)



## Goal is to answer the following:

6. What are risks and how are risks identified and rated?
7. What is the appropriate level of depth when assessing risk?
8. What are control activities and how are control activities determined to be sufficient?
9. When do corrective action plans need to be documented and what should be included?

(Slide 6)



(Slide 7)

**AGENCY RISK ASSESSMENT IMPLEMENTAION-(Maggie Garrett presenting)**



## Control Self-Assessment (CSA)

Defined by the Institute of Internal Auditors (IIA):

*“CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met.”*

Source: Professional Practices Pamphlet 98-2, A Perspective on Control Self-Assessment

(Slide 8)

In the General Overview workshop we discussed the definition of Agency Risk Assessment and said that it was 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; and, we focused on the fact that Agency Risk Assessment revolves around the achievement of objectives. In this presentation we want to discuss what the term “Control Self-Assessment” means and how that relates to the Agency Risk Assessment being performed.

To do that let’s take a look at the definition of Control Self-Assessment, which is also referred to as “CSA” (read slide).

Notice that this definition has a focus on achievement of objectives too. It has a very similar meaning compared to the definition of our Agency Risk Assessment.

What is the difference between the two?

## Difference in Terms

Control Self-Assessment	Agency Risk Assessment
<ul style="list-style-type: none"><li>• Term used by professional organizations, such as IIA.</li><li>• Includes different methods for implementation, such as facilitated meetings/workshops, questionnaires/surveys and management-produced analysis.</li><li>• Several options for workshop formats, which include objective-based, risk-based, control-based, process-based, situational approach.</li><li>• Doesn't specify a particular format for documentation.</li></ul>	<ul style="list-style-type: none"><li>• Term used by Arkansas State Agencies.</li><li>• Facilitated meetings/workshops are recommended.</li><li>• The risk-based approach workshop is used, which begins with identification of objectives.</li><li>• A specific format is used to document the control information.</li></ul>

(Slide 9)

This next slide shows a few of the differences between the terms (read slide).

So, really, Agency Risk Assessment is a form of Control Self-Assessment.



# Control Self-Assessment (CSA)

## Approach to Agency Risk Assessment

Workshops to facilitate communication

Agency initiated

Document results

Management determines if changes are needed

(Slide 10)

Here's what we mean when we say we are going to take the control self-assessment approach to Agency Risk Assessment: we mean that workshops (or brainstorming sessions) should be used to facilitate communication regarding risks, control activities and corrective action plans, that the process should be initiated by the agency, that the results should be documented and that management is responsible to make the final determination about any changes that should be made.

If you attended the General Overview presentation, you may remember that we discussed the two-year cycle recommended for this process and it was:

Once the objectives are identified then brainstorming sessions can be scheduled with all levels of employees to identify risks and control activities. 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, they will also determine the corrective action plan to implement with those documented in mind. Once this is concluded, a final document will show the current control activities in place and list any corrective action plans that cannot be implemented until a future date. 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.

What we are going to focus on for this presentation are the workshops or brainstorming sessions used in the control self-assessment method: how to conduct them, what to discuss, and tools and techniques that can be used to facilitate communication.

We will also be discussing the components of the Agency Risk Assessment for which management is responsible in an effort to assist with the organization and completion of the analysis and the document.



## Workshops

Organization of objectives is key

- Determine which employees are involved in accomplishing objectives
- Discuss and brainstorm risks and current control activities for one objective at a time unless the same group of employees is involved with more than one objective.

(Slide 11)

The purpose of the workshops/brainstorming sessions is to allow communication about risks and control activities between all levels of employees of the agency. The idea is to include input from all employees that work toward the same objective to give reasonable assurance that the objective will be achieved.

At this point, all objectives should already be determined. Management is responsible for determining the organization and the level of detail of all objectives. In planning the workshops, it should be considered that only the employees involved in achievement of the objectives that are going to be discussed be included in the meetings. Keep in mind that an employee whose work has nothing to do with the objective being discussed would be wasting their time if they were to be included. Thus, in scheduling the workshops the next step after the objectives have been set would be to determine which employees are involved in accomplishing the objective to be discussed.

We recommend discussing one objective at a time; unless, it would be beneficial to do otherwise. For example, smaller agencies (those that have a small number of employees) might be able to discuss all the objectives with all employees because all employees of the agency have a job duty that relates to every objective.

These workshops or brainstorming sessions should have a facilitator and recorder and we recommend limiting the number of participants to a group of 5-10.

# Workshops

Situation	Facilitator	Recorder
Small agency, groups can cover more than one objective within a workshop	Risk assessment coordinator	Risk assessment coordinator or someone in the meeting with good writing skills
Medium agency, some groups can cover more than one objective and some will only cover one objective	Risk assessment coordinator and agency management	Risk assessment coordinator and agency management or someone in the meeting with good writing skills
Large agency, most groups will only cover one objective within each workshop	Risk assessment coordinator, agency management, and internal audit	Risk assessment coordinator, agency management, and internal audit or someone in the meeting with good writing skills

(Slide 12)

It was mentioned in the General Overview presentation that DFA-IA had recommended that a “Risk Assessment Coordinator” be assigned within each agency when the requirement was first implemented back in 2004-5. It was intended that this individual be the point person for the Agency Risk Assessment process. This person would be the one to schedule brainstorming meetings, ensure that the Agency Risk Assessment document was completed by each department and pulled together into one document, work with management and be the liaison to DFA-IA regarding the document submission. (It was NOT intended that this person be responsible for the completion of the Agency Risk Assessment as a whole...it is management of the entire agency who is responsible for such.)

The person who is designated as the Risk Assessment Coordinator should be someone who is familiar with the agency and its structure and has the ability to discern and assist with identifying risks and control activities.

In the slide, you will notice that the Risk Assessment Coordinator is listed for each workshop situation as the facilitator and recorder. This is just to show that the Risk Assessment Coordinator can be such in each situation, it does not mean that this individual must be. It is the same for individuals in the other two positions mentioned; management and internal audit. The intent of this slide is simply to show that if one objective can only be discussed at a time and the groups are limited to 5-10 people that the Risk Assessment Coordinator will not be able to attend all meetings (especially in large agencies) to be the facilitator and/or recorder. Management or internal audit of the agency may be needed to assist in the brainstorming sessions.



# Workshops

Who should be a facilitator?

- Depends on the culture of the workshop group
- Choose a facilitator that would work best to accomplish the task
  - Agency Risk Assessment Coordinator
  - Agency Management
  - Internal Auditor

(Slide 13)

Who should be a facilitator? That depends upon the culture of the workshop group. The task is to encourage all levels of employees to contribute to the Agency Risk Assessment process. All levels of employees should bring to the table risks they are facing and discussion should be had about them. The facilitator should be the one that helps the group to stay on task and work through the relevant issues.

All levels of employees should be a part of recording the control activities that are currently in place. These are the control activities that will be showing in the control activities column of the Agency Risk Assessment document.

All levels of employees should give input as to the sufficiency of the control activities and be a part of brainstorming corrective action plans. All suggestions for corrective actions plans can be documented in the corrective action plan column. Management, (whoever is responsible for ensuring that the objective is achieved) will make the final determination about the sufficiency of the control activity and determine what changes will be implemented, if any. Management is responsible for ensuring that employees are trained properly if changes to job duties are needed. It is the facilitator's job during the workshop to ensure that participants understand that job duties do not change until management makes the decision to do so.

With this in mind, the facilitator should be someone who can accomplish the task at hand. Keep in mind that in some cases employees may be reluctant to share ideas if their boss is in the room. So it may be best for a manager to not attend the meeting in some cases. Some employees may be uncomfortable speaking with an "auditor" in the group. It just depends. What is important is that conversation and discussion about the topic is not hindered. So choose a facilitator that best fits the culture of the group.



## Workshops

Who should be a recorder?

- Someone with strong writing skills
- Someone who understands what needs to be documented
- Can be anyone

(Slide 14)

Who should be a recorder? Anyone can be a recorder that has good writing skills and understands what needs to be documented. We recommend that the brainstorming sessions be held in a room with a projection screen so that what is being recorded can be seen by the entire group. This will also help the group stay on task.

# Workshops

Be prepared

- Agenda with the task described
  - What is agency risk assessment
  - Why it's being done
  - What are objectives, risks, and control activities
  - What will happen to the results of the meeting

(Slide 15)

The facilitator should ensure that participants are prepared. We recommend sending an agenda with the task described in an email to all participants who will be attending a workshop. The questions listed on the slide are those that should be answered in the agenda email. Let's talk about one of the questions, "What will happen to the results of the meeting": the manager, who will be determining sufficiency of the control activities (this could be more than one manager) will review the document and determine if corrective action plans need to be implemented and if so which ones; and, after those are determined the final document will be sent to DFA-IA.



## Control Self-Assessment (CSA)

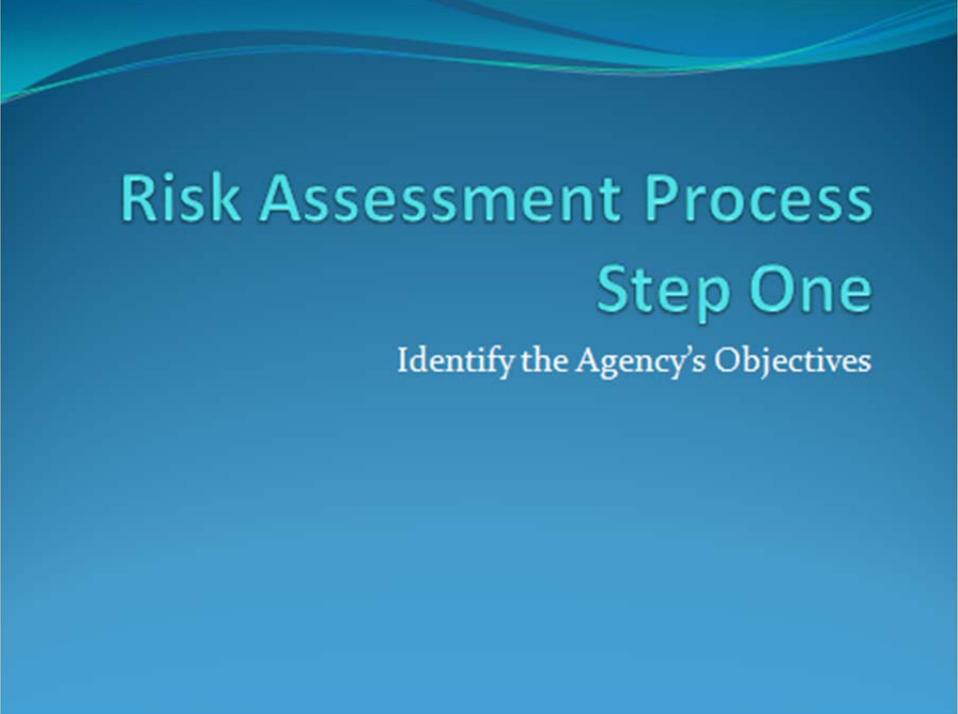
### Focus:

- Management determines objectives before workshops
- Workshops are conducted to determine risks and current control activities (document)
- Management determines sufficiency and makes final decision if control activities need to be changed (final document)
- Management communicates changes to employees
- Employees implement changes

(Slide 16)

Overall the control self-assessment approach means (read slide).

At this time Chandria Willis will talk about the components of the Agency Risk Assessment and give you some tools and techniques to use in the brainstorming sessions/workshops and to organize and complete the final document that will be sent to our office.



# Risk Assessment Process

## Step One

Identify the Agency's Objectives

(Slide 17)

**OBJECTIVES**-(Chandria Willis presenting)

The first step in the risk assessment process is the identification of the agency's objectives.

Which should come first? Objectives or risks?



*How do we know what controls we need to have in place if we don't know what we are trying to accomplish?*

(Slide 18)

There is a common misconception that the identification of risks should be the first step in the process; however, a more thorough process begins with the identification of objectives. Then, risks that may present a barrier to meeting each objective will be identified and the agency will be able to determine if there are sufficient controls in place to mitigate those risks. Think of it this way...how do we know what controls we need to have in place if we don't know what we are trying to accomplish?

## Organization first!!!

Before jumping in and beginning to identify your objectives, the risk assessment workbook needs to be organized.

1. The agency's name, department, activity, preparer, and date prepared will be listed at the top of each sheet.
2. Each tab in the risk assessment workbook will contain a different worksheet. The agency's size will determine the content of the worksheets.

(Slide 19)

Before jumping in and beginning to identify your objectives, the risk assessment workbook needs to be organized. The agency's name, department, activity, preparer, and date prepared will be listed at the top of each sheet. Each tab in the risk assessment workbook will contain a different worksheet. The size of the agency will determine the content of the worksheets.



## Spreadsheet Design

Each spreadsheet will contain the same columns:

- Objectives
- Risks
- Significance/impact
- Likelihood
- Control activities
- Management conclusion
- Corrective action plan

(Slide 20)

Each spreadsheet will contain the same columns: objectives, risks, significance/impact, likelihood, control activities, management conclusion, and corrective action plan. The column that we will focus on during this part of the presentation is the “objectives” column. All of the agency’s objectives will be listed in this column.

### Risk Assessment and Control Activities Worksheet

Agency: \_\_\_\_\_

Department: \_\_\_\_\_ Prepared By: \_\_\_\_\_

Activity: \_\_\_\_\_ Date Prepared: \_\_\_\_\_

Objective Type	Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities	Mgmt Conclusion	Corrective Action Plan New or Additional Control Activity
		Risks	Significance / Impact	Likelihood			

(Slide 21)

This is a screen-shot of the risk assessment worksheet. This worksheet will be used for every department and activity that is represented in your agency's risk assessment.

## Example—AR Department of Community Corrections

Large agencies may find it helpful to use a separate tab for each division of the agency. The Department of Community Corrections might list the following divisions as separate activities on different tabs of the workbook:

- Administration
- Parole & Probation Services
- Residential Services
- Public Relations
- Grievance Office
- Legal Services
- Internal Affairs

(Slide 22)

Large agencies will find it helpful to use a separate tab for each division of the agency. For example, the Arkansas Department of Community Correction may list the following divisions as separate activities on different tabs of the workbook: Residential Services, Parole & Probation Services, Residential Services, Public Relations, Grievance Office, Legal Services, and Internal Affairs. All of the administrative-type activities, such as payroll, purchasing, and cash receipts, would be listed on the “Administration” tab.

## Example—AR State Board of Massage Therapy

Smaller agencies will find it more appropriate to use a different tab for the actual activities that are performed in the agency. The Massage Therapy Board might list the following activities on separate tabs of the workbook:

- Receipts
- Disbursements
- Payroll
- Licensing
- Complaints
- Regulation

(Slide 23)

Smaller agencies will find it more appropriate to use a different tab for the actual activities that are performed in the agency. For example, the Arkansas State Board of Massage Therapy may list the following activities on different tabs of the workbook: Receipts, Disbursements, Payroll, Licensing, Complaints, and Regulation. These agencies will put “administration” on the line for “department” on each tab.

## What are objectives?

Objectives are the short-term goals that the organization wants to accomplish.



(Slide 24)

So, what are objectives? They are the short-term goals that the organization wants to accomplish.

## Objectives

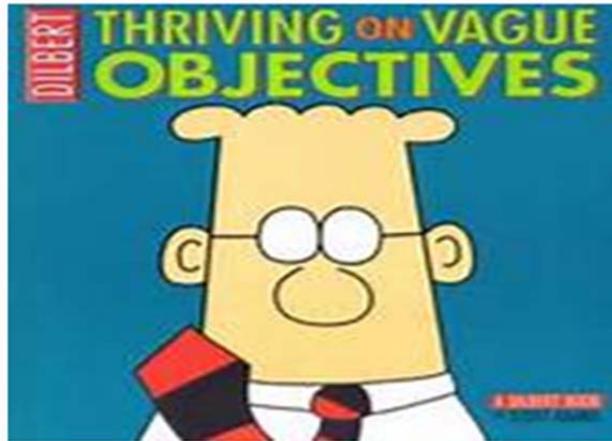
- The pieces that make up the agency's overall goals and mission.
- The things that the agency wants to accomplish within the next year.



(Slide 25)

They are the pieces that make up the agency's overall goals and mission. It is helpful to think of objectives as being the things that the agency desires to accomplish within the next year.

This is what we DON'T want...



(Slide 26)

When formulating your objectives, please make sure that they are not vaguely written.

## Objectives

- Specific and measurable
- Reflect the desired outcome, not the method that is used to accomplish the goal
- Can be both broad, relating to the agency's overall mission, and narrow, relating to an individual activity or section of the agency



(Slide 27)

Defining objectives that are specific and measurable to various levels of the agency is a crucial part of a successful risk assessment. Objectives should also reflect the desired outcome, not the method that is used to accomplish the goal. They **can** be broad, relating to the agency's overall mission, but they will more often be narrow, relating to an individual activity or section of the agency.

## Types of Objectives

According to COSO:

- Operational
- Reporting
- Compliance



(Slide 28)

It may be helpful for you to think about and identify your objectives based on objective type. According to COSO, there are three different categories of objectives: reporting, operational, and compliance.

## Operational Objectives

- Ensure that the agency's staff responds to citizens' problems and/or requests in a timely manner
- Ensure that the goals of each department are accomplished
- Should be identified for EVERY department within the agency (if there are no operational objectives for the department, there is no need for the department to exist)



(Slide 29)

Operational objectives ensure that the agency's staff responds to citizen's problems and/or requests in a timely manner and that the goals of each department are accomplished. Operational objectives should be identified for every department within the agency. Every department WILL have operational objectives. If there are no objectives for the department, there is no need for the department to exist.

## Reporting Objectives

- Ensure that the agency's reporting obligations are met accurately, timely, and completely.
- In the past, only addressed financial reporting, but currently include ALL types of reports, such as...
  - Reports that are required by the DFA CAFR section, reports that are required by granting organizations, reports that are required by Boards or Commissions, and any other reporting requirements that may be placed on the agency.



(Slide 30)

Reporting objectives pertain to the preparation of required financial and/or performance-related reports. In the past, this category of objectives only related to financial reporting requirements. COSO revised its framework in 2013; however, and the definition was revised to include all types of reporting obligations. Therefore, this type of objective will include reports that are required by the DFA CAFR section, reports that are required by granting organizations, reports that are required by Boards or Commissions, and any other reporting requirements that may be placed on the agency.

## Compliance Objectives

- Ensure that the agency abides by all applicable laws and statutes, including federal, state, and local laws
- Ensure that the agency abides by all grant requirements
  - These will be specified in the grant award documents
- Include internally-generated policies & procedures
  - A requirement may not be required by law, but if it is required by the agency's internal policies, it can be linked to a compliance objective



(Slide 31)

Compliance objectives ensure that the agency abides by all applicable laws and statutes. This includes federal, state, and local laws. Compliance objectives also include the requirements of any grants that the agency may receive. Grant award documents usually identify the goals or objectives of the grants. In addition to these legal requirements, compliance objectives include internally-generated policies and procedures. Although a particular activity may not be required by law, if it is required by the agency's internal policies, it can be linked to a compliance objective.

## How are objectives formed?

Objectives should reflect the desired outcome, rather than state the method that will be used to meet the goal. In order to ensure that the objectives are properly formed, it is helpful to ask the following questions:

1. Does it relate to the agency's goals or mission?
2. Can it be measured?
3. Is there an end result?



(Source: Control Self-Assessment: A Practical Guide, Hubbard 2005)

(Slide 32)

### ***How are objectives formed?***

The objectives should reflect the desired result, rather than state the method that will be used to meet the objective. In order to ensure that the objectives are properly formed, it is helpful to ask the following questions:

1. Does it relate to the agency's goals or mission?
2. Can it be measured?
3. Is there an end result?

## Whose responsibility is all of this?

### Management!!!

- What are you trying to accomplish?
- What do you want your employees to do in order to help you accomplish these things?



(Slide 33)

Objectives should be developed by management. What are you trying to accomplish? What do you want your employees to do in order to help you accomplish these things? These are the questions that you should ask yourself when attempting to identify the agency's objectives.

## Objectives

- Objectives should be developed for each department within the agency.
- High-level organizational objectives may not apply equally to each department, but each department will have a variety of objectives.
- Objectives often begin with the words, “to ensure,” because they reflect a desired outcome.

(Slide 34)

Objectives should be developed for each department within the agency. High-level organizational objectives may not apply equally to each department, but each department will have a variety of objectives. High-level organizational objectives will usually be listed on the “administration” tab of the risk assessment.

Objectives often begin with the words, “to ensure,” because they reflect a desired outcome.



## Objectives

Objectives should not be worded as though they are processes or procedures; they should be worded as goals that the agency desires to meet. In order to separate an objective from a way to achieve the objective, you may ask:

1. Is it a desired result?
2. Is it a how (way to achieve) or a what (objective)?
3. Is it a “means” or an “end?”

(Slide 35)

Objectives should not be worded as though they are processes or procedures; they should be worded as short-term goals that the agency desires to meet. In order to separate an objective from a way to achieve the objective, you might ask:

1. Is it a desired end result?
2. Is it a how (way to achieve) or a what (objective)?
3. Is it a “means” or an “end?”

## Example—Improperly Worded Obj.

To ensure that management approves all timesheets.

1. Is it a desired end result?

No. This is a step in the payroll process.

2. Is it a “how” or a “what”?

This is a “how.” It’s a way to achieve an objective, rather than an actual objective.

3. Is it a “means” or an “end”?

This is a means. As previously stated, this is a step in the payroll process. It is not the end result of the process.

(Slide 36)

The following is an example of this concept:

Improperly worded objective: To ensure that management approves all timesheets.

1. Is it a desired end result?

a. No. This is a step in the payroll process, not the end result.

2. Is it a how or a what?

a. This is a how. It’s a way to achieve an objective, rather than an actual objective.

3. Is it a means or an end?

a. This is a means. As previously stated, this is a step in the payroll process. It is not the end result of the process.

So, what would be a better way to word this objective?

## Example—Properly Worded Obj.

To ensure that payroll is accurately processed.

1. Is it a desired end result?

Yes. The desired short-term goal, or objective, is for payroll to be processed accurately.

2. Is it a “how” or a “what”?

This is a “what.” It is stating what we desire to achieve. It doesn’t tell us how we are going to achieve it.

3. Is it a “means” or an “end”?

This is an end. The means will be the various control activities that are in place. The end result is that payroll is processed accurately.

(Slide 37)

Answer: To ensure that payroll is accurately processed.

Let’s go through the same questions, using this objective:

1. Is it a desired end result?

a. Yes. The desired short-term goal, or objective, is for payroll to be processed accurately.

2. Is it a how or a what?

a. This is a what. It is stating what we desire to achieve. It doesn’t tell us how we are going to achieve it.

3. Is it a means or an end?

a. This is an end. The means will be the various control activities that are in place. The end result is that payroll is processed accurately.

## Where do we start?

A good starting place for identifying the agency's objectives is the mission statement. The mission statement will contain the overall purpose of the agency and/or the goals that the agency is attempting to achieve.



(Slide 38)

A good starting place for identifying the agency's objectives is the agency mission statement. The mission will contain the overall purpose of the agency and/or the long-term goals that the agency attempts to achieve.

# Arkansas Department of Workforce Services

*To enable the Arkansas workforce to compete in the global economy by linking a comprehensive array of services for employers and job seekers.*



(Slide 39)

The mission of the Arkansas Department of Workforce Services is: To enable the Arkansas workforce to compete in the global economy by linking a comprehensive array of services for employers and job seekers. (<http://dws.arkansas.gov/About/index.htm>)

## How do we develop objectives, based on this mission statement?

1. Each goal that is identified within the mission statement should be reviewed.
  - To provide services that enable the Arkansas workforce to compete in the global economy.
  - To provide a comprehensive array of services that are beneficial to employers and job seekers.
2. Think of all of the objectives that will need to be met in order to meet these goals. What will it take to ensure that these goals are met?
  - Sufficient funds to provide the services, competent staff, technological resources, materials & supplies, etc.

(Slide 40)

In order to develop objectives that are based upon this mission statement, each goal that is identified within the mission statement should be reviewed:

1. To provide services that enable the Arkansas workforce to compete in the global economy.
2. To provide a comprehensive array of services that are beneficial to employers and job seekers.

Next, think of the objectives that will need to be met in order to meet these goals. What will it take to ensure that these goals are met? The agency will need funds available to provide the services, competent staff, technological resources, the appropriate materials and supplies, etc. The list could go on and on.



What objectives can be formed from the mission statement of the Department of Workforce Services?



(Slide 41)

## Arkansas Department of Workforce Services

*To enable the Arkansas workforce to compete in the global economy by linking a comprehensive array of services for employers and job seekers.*

**DWS**  
Department of Workforce Services

*"Making strides from good to Great!"*  
-Artee Williams, DWS Director



(Slide 42)



**Mission:**  
To enable the Arkansas workforce to compete in the global economy by linking a comprehensive array of services for employers and job seekers.

**Objectives:**

1. To ensure that the agency hires and promotes qualified employees.
2. To ensure efficient use of budgeted funds.
3. To ensure that all purchases are made in accordance with Arkansas procurement law.
4. To ensure that program XYZ is properly administered.

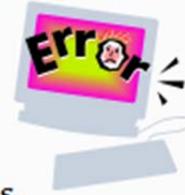
(Slide 43)

The following are examples of possible objectives that could be formed from this mission:

- To ensure that the agency hires and promotes qualified employees.
- To ensure efficient use of budgeted funds.
- To ensure that all purchases are made in accordance with Arkansas procurement law.
- To ensure that program XYZ is properly administered.

Please note that the fourth example includes the title of a specific program. If your agency is responsible for overseeing or administering various programs, there should be a separate objective included for each program.

## Common Errors



- Failing to consider various types of objectives.
- Failing to consider the relationship between objectives, to ensure that they don't conflict with each other.
- Attempting to apply high-level organizational objectives to each department.
- Wording the objectives so narrowly that risks cannot be properly identified.

(Slide 44)

The following are common errors that are made when attempting to identify objectives:

- Failing to consider various types of objectives.
- Failing to consider the relationship between objectives, to ensure that they don't conflict with each other.
- Attempting to apply high-level organizational objectives to each department.
- Wording the objectives so narrowly that risks cannot be properly identified.



## Responsibility

The identification of objectives is the responsibility of **management**.

It is the responsibility of the **risk assessment coordinator** to assist management by ensuring that a thorough list of objectives has been considered. This can be done by reviewing the following sources...

(Slide 45)

It was previously stated that the identification of objectives is the responsibility of management. However, it is the responsibility of the risk assessment coordinator to assist management by ensuring that a thorough list of objectives has been considered.

It is recommended that the risk assessment coordinator review the following sources and determine if there appear to be any objectives that have been omitted from the risk assessment, prior to submitting the risk assessment to Internal Audit.



## Sources



- Rules and Regulations
  - What is required of the agency? Are there specific mandates that must be adhered to? Is there new legislation that will result in significant changes?
- Agency Website
  - Often contains a plethora of information, some of which can be used to identify additional objectives.
- Agency Budget
  - In what areas does the agency spend the majority of its funds?
- Grant Award Documents
  - What is the goal of the grant? Are there performance requirements? Reporting requirements?

(Slide 46)



## Sources



- Strategic Plan
  - What are the agency's short-term goals?
- Organizational Chart
  - What are the purposes of the various departments within the agency?
- Agency staff
  - What does staff perceive their purpose to be within the agency?

(Slide 47)

# EXAMPLES



*Need a helping hand?*

(Slide 48)

Now we will give you a helping hand, and provide examples of each type of objective that has been discussed.

## Reporting Objectives

- To ensure that federal grant reporting for XYZ Grant is complete, accurate, and timely.
- To ensure that all money collected on behalf of the State from racing and gaming activities is accurately reported.
- To ensure that the Treasurer's Office's Local Tax Distribution Report is prepared accurately and timely.

(Slide 49)

A few examples of reporting objectives are:

- To ensure that federal grant reporting for Grant XYZ is complete, accurate, and timely.
  - This objective is rather broad. Grants often have both financial reporting requirements and performance reporting requirements. If you are able to address all of the reporting requirements under this objective, as written, then it is acceptable to word the objective in this manner. If there are different groups of people working on the fiscal and programmatic aspects of the grant, it may be better to have separate objectives for each type of reporting requirement.
  - There should be separate objectives for each grant that the agency receives.
- To ensure that all money collected on behalf of the State from racing and gaming activities is accurately reported.
- To ensure that the Treasurer's Office's Local Tax Distribution Report is prepared accurately and timely.



## Operational Objectives

- To ensure that payroll is processed accurately and timely.
- To ensure that fixed assets are safeguarded.
- To establish a culture of honesty and ethical behavior within the agency.
- To issue licenses to qualified applicants in a timely manner.
- To litigate workers' compensation claims in a timely and professional manner.

(Slide 50)

The following are a few examples of operational objectives:

- To ensure that payroll is processed accurately and timely.
- To ensure that fixed assets are safeguarded.
- To establish a culture of honesty and ethical behavior within the agency.
  - Note: This is an agency-wide objective that would be included on the “administration” tab of the risk assessment.
- To issue licenses to qualified applicants in a timely manner.
- To litigate workers' compensation claims in a timely and professional manner.

## Compliance Objectives

- To promulgate rules and regulations as required by new legislation.
- To ensure that hearing decisions are made in accordance with the law.
- To ensure that Grant XYZ complies with the Davis-Bacon Act.

(Slide 51)

The following are a few examples of compliance objectives:

- To promulgate rules and regulations as required by new legislation.
- To ensure that hearing decisions are made in accordance with the law.
- To ensure that Grant XYZ complies with the Davis-Bacon Act.
  - If there are several compliance requirements that are applicable to a particular grant, it may be better to form a separate objective for each requirement. If you believe that you can address all of the compliance requirements in one objective, you can word the objective as follows: To ensure that Grant XYZ complies with all applicable federal grant compliance requirements.
  - As previously stated, please form a separate objective or set of objectives for each grant that the agency receives.

# Questions?



(Slide 52)

***In conclusion, please remember:***

- Identifying objectives is the first step in the risk assessment process.
- Objectives are short-term goals that the agency wants to accomplish.
  - Defining objectives that are specific and measurable to various levels of the agency is a crucial part of a successful risk assessment.
- There are three categories of objectives: reporting, operational, and compliance.
- Objectives can be obtained from a variety of sources, including the agency's mission statement and website.

# What's Next?

## Identification of Risks



(Slide 53)

The next step in the risk assessment process is the identification of risks that may impede the achievement of the agency's objectives.



(Slide 54)



(Slide 55)

**RISKS**

## Organization first!!!

When reviewing the risk assessment, it is important to be able to clearly determine which risks are related to each objective.

- Some objectives may have more risks than others, but at least one risk should be associated with each objective.
- Risks will be listed under the column that is entitled, “risks.”
- Some objectives may share similar or identical risks.

(Slide 56)

Now that you have organized your workbook and identified your objectives, it is time to focus on the identification of the agency’s risks. Risks should be identified for each objective. Some objectives may have more risks than others, but at least one risk should be associated with each objective.

Risks will be listed next to the associated objective, in the column that is entitled “Risks.” Some objectives may share similar or identical risks.

**Risk Assessment and Control Activities Worksheet**

Agency: \_\_\_\_\_

Department: \_\_\_\_\_ Prepared By: \_\_\_\_\_

Activity: \_\_\_\_\_ Date Prepared: \_\_\_\_\_

Objective Type	Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities	Mgmt Conclusion	Corrective Action Plan New or Additional Control Activity
		Risks	Significance / Impact	Likelihood			
	Accurate and timely processing of payroll.	Employee is paid for inaccurate number of hours.					
	Hiring qualified employees.	Employee uses leave that is not earned. Unqualified personnel are hired.					

(Slide 57)

The organization of the risk assessment is important. This process is meant to be a useful tool for the organization. In order to be useful and effective, the tabs on the spreadsheet must be organized in a manner that is easy to follow and understand.

This slide lists two different objectives, both related to agency administration. The objectives are listed in the “objectives” column. Each risk that relates to the stated objective is listed in the “risk” column. Note that the risks that relate to the first objective, “accurate and timely processing of payroll,” are listed next to that objective. The risks that relate to the second objective, “hiring qualified employees,” are listed next to that objective. It is easy to determine which risks relate to each objective.

# What is a risk?

A risk is anything that may prevent the agency from meeting its objectives.



(Slide 58)

A risk is anything that may prevent the agency from meeting its objectives.

## Are risks always fraud-related?

Some people think of risks as only being related to fraud, but risks are ANYTHING that can prevent an objective from being met.



**RISK**  
happens!

(Slide 59)

Some people think of risks as only being related to fraud, but risks can be much more than that. Anything that can prevent an objective from being met is a risk.

## Examples

### Cash receipts are stolen.

- Affects cash
- Constitutes fraud
- Immediately impacts the agency



### Quarterly revenue estimations are not met.

- Affects cash
- Can result from any number of reasons (fraud, budget cuts, over-zealous revenue projections, etc.)
- Will impact the agency if it continues to occur each quarter



(Slide 60)

Consider the following risks:

- Cash receipts are stolen.
- Quarterly revenue estimations are not met.

Both are risks that affect cash; however, only one is fraud-related. It is disappointing to fail to maximize your revenue, resulting in your agency not meeting its revenue estimations for the quarter. If this occurs each quarter, for an extended period of time, it could even affect operations. However, the occurrence of this risk does not mean that fraud has occurred. This does not mean that it is not a valid risk. An occurrence does not have to be the result of fraudulent activities in order to be a risk. A risk is anything that could prevent an objective from being met. For example, if the objective is to maximize revenue, then anything that will prevent this from occurring is a risk.

## How are risks identified?

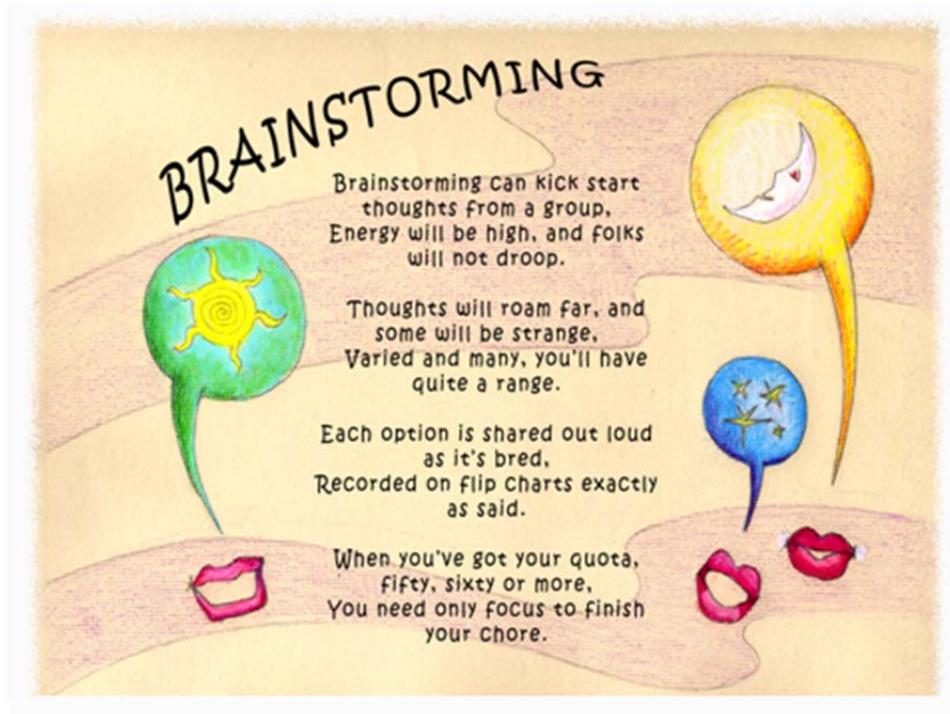


- Organized by objective
- Separate sessions for management and line-level employees
- Limited to 5-10 people

(Slide 61)

In order to thoroughly identify the agency's risks, it is recommended that you conduct a brainstorming session with employees from each level of the organization. Each level of employees, from line-level to upper management, will be able to identify things that will prevent them from being effective in their jobs. If the brainstorming session is organized by objective, it will be easier to ensure that the list of risks that is compiled is thorough.

It is recommended that large agencies conduct separate brainstorming sessions, in order to be more effective and efficient. If management isn't on board, it may be better for the risk assessment coordinator to conduct a one-on-one session with each manager. If management is on board, the brainstorming sessions can be conducted by rank within the agency. There should be separate sessions for management and line-level employees. The optimal size is 5-7 people, but each session should definitely be limited to ten people, in order to be effective.



(Slide 62)

This is a cute poem about brainstorming. We don't expect you to have 50-60 risks at the end of your brainstorming sessions, but you should have a very thorough list.

## Methods to use to organize the brainstorming session:

- Review the following tools on the DFA Office of Accounting Internal Audit website: Comprehensive Example—Department of Labor, Financial & Administrative General Risks Spreadsheet, and the Service Bureau Risk Assessment Template.
- Review a list of general risks for each objective to decide if any of the risks apply. If the risks apply, they can be revised to be more specific or to be more in line with the objective.
- Utilize the Association of Government Accountants (AGA)'s Fraud Prevention Toolkit.

(Slide 63)

The following are a few examples of methods that can be used during your brainstorming sessions, in order to get the ideas flowing:

- Review the DFA Office of Accounting Internal Audit website (<http://www.dfa.arkansas.gov/offices/accounting/internalaudit/Pages/RiskAssessment.aspx>) for the following tools:
  - Comprehensive Example—Department of Labor
    - There may be risks present that are applicable to your agency.
  - Financial and Administrative General Risks Spreadsheet
    - This spreadsheet provides examples of general risks for the following areas: environment, cash receipts, cash disbursements, procurement, payroll, accounts receivable, investments, grants, inventory, financial reporting, and AASIS access.
  - Service Bureau Risk Assessment Template
    - There will be risks present that will be applicable to most service bureau agencies.
- Review a list of general risks for each objective to decide if any of the risks apply. If the risks apply, they can be revised to be more specific or to be more in line with the objective.
- Utilize the Association of Government Accountants (AGA)'s Fraud Prevention Toolkit.

These are only examples. If you have other methods that you would like to use, please feel free to do so.

## Review a list of general risks for each objective

- Incorrect records and/or information
- Unacceptable accounting practices
- Legal action
- Non-compliance of new laws
- Service interruption (disaster, technological issues, etc.)
- High costs
- Unrealized or lost revenue
- No appropriation for needs
- Loss or destruction of assets
- Public dissatisfaction
- Conflict of interest
- Fraud



Source: Control Self-Assessment: A Practical Guide, Hubbard 2005

(Slide 64)

This is a list of general risks that can be reviewed for each objective. If these risks apply, they can be revised to be more specific or to be more in line with the objective.

- Incorrect records and/or information
- Unacceptable accounting practices
- Legal action
- Non-compliance of new laws
- Service interruption (disaster, technology issues, etc)
- High costs
- Unrealized or lost revenue
- No appropriation for needs
- Loss or destruction of assets
- Public dissatisfaction
- Employee dissatisfaction
- Conflict of interest
- Fraud

This is not a comprehensive list, but it covers many general areas and will be applicable to most agencies. It is a great starting point when attempting to identify risks.

## Risks—Exercise 1

Objective: To ensure that payroll is processed accurately and timely.

Review the list of general risks, and determine if each risk can apply to the objective. If the risk applies, check the “yes” box. If it does not apply, check the “no” box.

(Slide 65)

The following is an example of how to use this list in a brainstorming session:  
Let's use an objective that will apply to every agency; one that is related to payroll.

Objective: To ensure that payroll is processed accurately and timely.

## General Risks

- Incorrect records and/or information
- Unacceptable accounting practices
- Legal action
- Non-compliance of new laws
- Service interruption (disaster, technological issues, etc.)
- High costs
- Unrealized or lost revenue
- No appropriation for needs
- Loss or destruction of assets
- Public dissatisfaction
- Conflict of interest
- Fraud

(Slide 66)

Review each risk on the list, as it relates to accurate and timely payroll processing. Begin by thinking about whether or not the item is a valid risk, based upon the objective. Then, determine if you need to re-word the risk or if there are related risks that should also be considered.

Answer: Each general risk on the list could possibly be associated with the objective, with the exception of one: Public dissatisfaction. (Employees would not be satisfied if their paychecks were inaccurate or late, but the public would not be affected.)



## AGA Fraud Prevention Toolkit

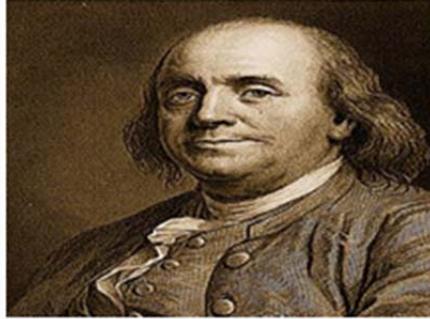
A tool that can be used by government employees to help identify fraud-related risks and red flags.

*(Note: It also contains tools and best practices that can help to identify or develop internal controls, but we will take a look at those later in the workshop.)*

(Slide 67)

Another method that you may find helpful is to utilize the Association of Government Accountant (AGA)'s Fraud Prevention Toolkit. This is a tool that can be used by government employees to help identify fraud-related risks and red flags. It also contains tools and best practices that can help to identify or develop controls, but we will take a look at those when we discuss control activities.

*“There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government.”*



(Slide 68)

Ben Franklin said it best, “There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government.”

## Why is this toolkit necessary?

- The typical organization loses five percent of its annual revenue to fraud.
- Governments are the second most frequent victims of fraud (after banking)
- The median duration of those fraud schemes that are discovered is 18 months
- Nearly half of victim organizations do not recover any losses that they suffer due to fraud

*(Statistics obtained from the Association of Certified Fraud Examiners' 2012 Report to the Nations)*

(Slide 69)

AGA decided that this toolkit was needed after reviewing the Association of Certified Fraud Examiner's 2012 Report to the Nations. According to their findings:

- The typical organization loses five percent of its annual revenue to fraud.
- Governments are the second most frequent victims of fraud (after banking)
- The median duration of those fraud schemes that are discovered is 18 months
- Nearly half of victim organizations do not recover any losses that they suffer due to fraud

## AGA Fraud Prevention Toolkit

1. Go to AGA's national webpage: [www.agacgfm.org](http://www.agacgfm.org).
2. Select "Tools & Resources." A list of the toolkits that AGA has developed will be provided.
3. Select "Fraud Prevention Toolkit."

(Slide 70)

In order to access the Fraud Prevention Toolkit, go to AGA's national webpage. [www.agacgfm.org](http://www.agacgfm.org). Select "Tools & Resources." A list of the toolkits that the organization has developed will be shown. Select the "Fraud Prevention Toolkit."

**AGA**  
Partnership for Intergovernmental  
Management and Accountability

# The AGA Fraud Prevention Toolkit

An AGA Intergovernmental Partnership Project

Welcome to the AGA Fraud Prevention Toolkit!

**View Fraud Prevention Tools by:**

- Business Process
- Program Area
- Fraud Type
- Fraud Awareness and Mitigation
- Tools/Best Practices
- Fraud News
- Glossary of Terms
- About the Toolkit
- How to Use the Toolkit

**Search for Fraud Prevention Tools by:**

Google™ Custom Search

AGA's Fraud Prevention Toolkit provides current, state-of-the-art tools for federal, state, local and tribal government financial managers to use in preventing and detecting fraud. It furthers AGA's mission of "Advancing Government Accountability."

AGA convened a special work group of government officials to develop this Toolkit because:

- The typical organization loses 5 percent of its annual revenue to fraud.
- Governments are the second most frequent victims of fraud (after banking).
- The median duration of those fraud schemes that are discovered is 18 months.
- Nearly half of victim organizations do not recover any losses that they suffer due to fraud.

*Source: Association of Certified Fraud Examiners' 2012 Report to the Nations*



**"There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government."**

- Ben Franklin

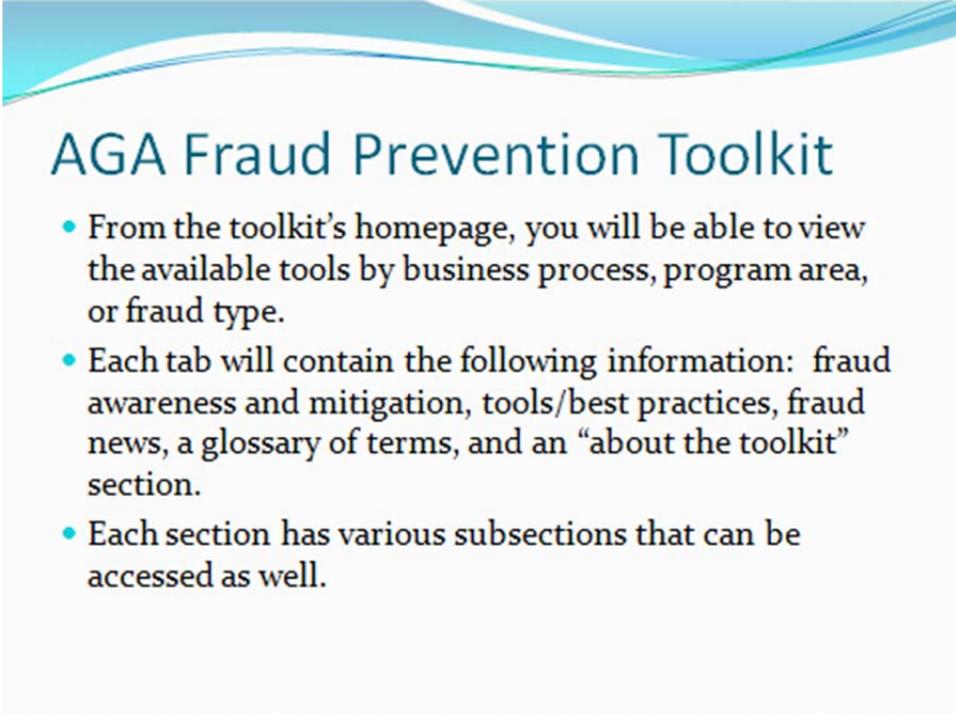
The Toolkit is organized in a manner that promotes education. It contains a comprehensive array of tools, posters, educational materials, PowerPoint Presentations and videos. Users can find tools by looking under business process such as accounts receivable, program areas like the Office of Management and Budget's high-risk programs, or by fraud type such as **Bid Rigging**.

**Toolkit Features:**

- Quick summaries of types of fraud likely to be encountered by managers

(Slide 71)

This is a screen-shot of the toolkit's homepage.

The slide features a decorative header with blue and white wavy lines. The title "AGA Fraud Prevention Toolkit" is centered in a dark blue font. Below the title is a bulleted list of three items, each starting with a blue circular bullet point. The text is in a black, sans-serif font.

## AGA Fraud Prevention Toolkit

- From the toolkit's homepage, you will be able to view the available tools by business process, program area, or fraud type.
- Each tab will contain the following information: fraud awareness and mitigation, tools/best practices, fraud news, a glossary of terms, and an "about the toolkit" section.
- Each section has various subsections that can be accessed as well.

(Slide 72)

From the toolkit's home page, you will be able to view the available tools by business process, program area, or fraud type. Each of these tabs will contain the following information: fraud awareness and mitigation, tools/best practices, fraud news, a glossary of terms, and an "about the toolkit" section. Each of these sections has various subsections available that can be accessed.

**View Fraud Prevention Tools by:**

Business Process	Program Area	Fraud Type
Fraud Awareness and Mitigation		
Tools/Best Practices		
Fraud News		
Glossary of Terms		
About the ToolKit		
How to Use the ToolKit		

The screenshot shows the AGA Fraud Prevention ToolKit website. The navigation menu on the left is highlighted with a red box. The main content area includes a search bar and introductory text about the toolkit's purpose. The text mentions that the toolkit provides current, state-of-the-art tools for federal, state, local and other government financial managers to use in preventing and detecting fraud, in furtherance of their mission of advancing government accountability.

(Slide 73)

This is a screen-shot of the various sections that are available.

## Tools by Business Process

- Accounts payable
- Accounts receivable
- Contract management
- Grants and program management
- Payroll and human resources
- Procurement and purchasing
- Vendor debarment

(Slide 74)

We'll begin by looking at the tools by business process tab. The available business processes are: accounts payable, accounts receivable, contract management, grants and program management, information technology and security, inventory management, management, payroll & human resources, procurement/purchasing, and vendor debarment.

You can select any of these areas and access risks, red flags, and tools/best practices for the area.



## Example: Payroll/human resources tools

If you select the link for Payroll & Human Resources, you will be provided with a table that lists risks, red flags, and tools/best practices for this business area.

We will review the information that is provided for the risk of creating “ghost employees.”

(Slide 75)

We will look at the tools for the payroll and human resources section because payroll fraud is a type of fraud that every agency is susceptible to.

Payroll fraud can range from simple schemes, such as being paid for time not worked, to more complicated schemes, such as creating “ghost” employees. Let’s look at the information that is presented for the risk of ghost employees. Although it would be difficult for someone in a state agency to create a ghost employee, it is possible.

## Red flags related to “ghost employees”

- No evaluations, raises, or promotions over an extended period of time.
- Terminated employee is still on the payroll.
- Payments to employees not on employee master file.
- Employees with duplicate addresses, checking accounts, or social security numbers.
- Employees with no withholding taxes, insurance, or other normal deductions.
- Employees with PO boxes, drop box addresses, an organization's address, a prison address, or no home address.
- Unusual work location or no work phone.
- No annual/sick leave used over a reasonable period.

(Slide 76)

Red flags that may indicate that an individual who is on the payroll does not actually work at the agency are:

- No evaluations, raises, or promotions over an extended period of time
- Terminated employee is still on the payroll
- Payments to employees not on employee master file
- Employees with duplicate addresses, checking accounts, or social security numbers
- Employees with no withholding taxes, insurance, or other normal deductions
- Employees with PO boxes, drop box addresses, an organization's address, a prison address, or no home address
- Unusual work location or no work phone
- No annual/sick leave used over a reasonable period

The purpose of reviewing the red flags that are presented is to help you to determine if the red flags are related to activities that should be addressed in the risk assessment. The red flags could trigger discussions that may help you to identify additional risks and/or additional areas of concern.

## Do these red flags indicate fraud?

### It depends...

- There are AASIS controls that will prevent an employee from being paid without having a master data file created, but agencies who do not use AASIS may find this to be a valid red flag or risk.
- An unusual work location or no work phone may seem to be irrelevant when dealing with state agencies, but there are one-person boards and commissions for which the only employee works out of his/her home.

(Slide 77)

Also, I just want to note that the existence of these red flags does not necessarily constitute fraud, but they are indicators that additional review may be needed. There are AASIS controls that will prevent an employee from being paid without having a master data file created, but agencies who do not use AASIS may find this to be a valid red flag or risk. An unusual work location or no work phone may seem to be irrelevant when dealing with state agencies, but there are one-person boards and commissions for which the only employee works out of their home. There is no office location. The work phone is the employee's home phone. The employee lives in a small town that is barely a blip on the map. In these instances, it is the board's responsibility to provide oversight to ensure that fraud does not occur. The amount of money that flows through these small agencies may not be material to the state as a whole, based on dollar amount, but any misappropriation of taxpayer dollars is wrong, regardless of the amount.

As public servants, it's our responsibility to safeguard the state's assets.



## Using the toolkit during brainstorming

- Review each risk table that applies to the objective that you are discussing.
- Determine if any of the risks listed are valid risks for your agency.
- Discuss the risks that are listed to determine if there are additional risks that you should consider.

(Slide 78)

If you choose to use the toolkit during your brainstorming sessions,

- Review each risk table that applies to the objective that you are discussing.
- Determine if any of the risks listed are valid risks for your agency.
- Discuss the risks and red flags that are listed to determine if there are additional risks that you should consider.



*If there are tools or information that is available online that can assist you in your brainstorming sessions, use them!*

(Slide 79)

Don't reinvent the wheel. If you find other tools that will be helpful to you in your brainstorming sessions, use them.

## Common misconception

*An event is not a risk if it is well-controlled.*



(Slide 80)

One common misconception when identifying risks is to think that an event is not a risk, simply because it is well-controlled.

## Scenario

- There are three employees involved in the cash receipting process.
- Employee #1 is responsible for opening the mail and receipting all payments and employee #3 monitors this process.
- Employee #2 is responsible for making the bank deposit.
- Employee #3 is responsible for performing a reconciliation each month, to ensure that all funds that were received were properly deposited.
- All employees are properly trained and are bonded.

(Slide 81)

Consider the following scenario: There are three employees involved in the cash receipting process. Employee #1 is responsible for opening the mail and receipting all payments and Employee #3 monitors this process. Employee #2 is responsible for making the bank deposit. Employee #3 is responsible for performing a reconciliation each month, to ensure that all funds that were received were properly deposited. All three employees are properly trained and are bonded.

Assume that these are sufficient control activities for risks related to the cash receipt process.

## Question

Is there a risk that cash receipts will be stolen?



(Slide 82)

Since this process is well-controlled, is there a risk that cash receipts will be stolen?

## Answer



When you are identifying risks, do not be tempted to eliminate potential risks from the list simply because there are internal controls in place. At this point in the risk assessment process, focus on risks, not control activities.

(Slide 83)

Some people may say “no”, but the correct answer is “yes”. When you are identifying risks, do not be tempted to eliminate potential risks from the list simply because there are internal controls in place. At this point in the risk assessment process, the focus is on risks, not control activities.

Later in the presentation we will discuss that management will conclude if the control activities are sufficient for risks. This is where it is determined if the risk is managed appropriately.



## Examples

There are several risks that are common to all agencies. The following are examples. Because risks are things that will prevent an agency from meeting its objectives, the objective is listed first in each example.

*Note: There is not a comprehensive list of risks for each objective that will be presented. These are only a few examples of potential risks that will apply to each agency.*

(Slide 84)

There are several risks that are common to all agencies. The following are examples. Because risks are things that will prevent an agency from meeting its objectives, the objective is listed first in each example. There is not a comprehensive list of risks for each objective that is listed. These are simply a few examples of risks that will apply to almost everyone who has a desire to meet the stated objective.

Note: No narrative accompanies the slides that list examples.



If your agency issues licenses, you will have the following risks, regardless of the type of license that is being issued:

**Objective:** To issue licenses and renewals to persons who meet all of the licensing requirements.

**Risks:**

- Licenses are issued to unqualified applicants.
- License fees are not applied to the correct account.
- Fraudulent information or documentation is received from the applicant.

(Slide 85)



If your agency has employees, you will have the following risks:

**Objective:** To ensure that payroll is processed accurately and timely.

**Risks:**

- Employee is paid for an inaccurate number of hours.
- Employee uses leave that is not earned.
- Terminated employee continues to receive payment.

(Slide 86)



If your agency collects cash, you will have the following risks:

**Objective:** To ensure that cash receipts are processed accurately and timely, in accordance with agency policies, the Financial Management Guide, and applicable state laws.

**Risks:**

- Cash receipts are lost or stolen.
- Cash receipts are not recorded.

(Slide 87)



If your agency makes purchases, you will have the following risks:

**Objective:** To ensure that all purchases are made in accordance with state procurement laws.

**Risks:**

- Unauthorized purchases are made.
- Disbursements are made before goods are received.
- Disbursements are made to fictitious vendors.

(Slide 88)



If your agency has fixed assets, you will have the following risks:

Objective: To ensure that there is adequate control over all fixed assets.

Risks:

- Fixed assets are lost or stolen.
- Fixed assets are not tagged when they are acquired.

(Slide 89)



If your agency stores secure data on computers, you will have the following risks:

Objective: To ensure that there is adequate IT security for all sensitive and/or confidential information.

Risks:

- Employees share passwords.
- Data files are lost.
- Unauthorized personnel gains access to secure data.

(Slide 90)



If your agency desires an ethical workplace, you will have the following risks:

**Objective:** To establish a culture of honesty, integrity, and ethical operations.

**Risks:**

- A culture of honesty is not established.
- Employees are not aware of their ethical responsibilities.
- Employees are not aware of how to report unethical behavior.

(Slide 91)



If your agency is responsible for investigating complaints, you will have the following risks:

**Objective:** To ensure that all complaints are investigated and resolved in accordance with the Administrative Procedures Act.

**Risks:**

- All complaints are not investigated.
- Complaints are not investigated timely or thoroughly.
- The investigator is biased.

(Slide 92)

## Agency-specific risks

The following are a few examples of risks that are agency-specific. The agency's name and related objective are included, so that the relationship between the objective and risk can be observed. It is important that you **think outside the box** in order to generate a thorough list of risks for your agency.



(Slide 93)

The following are a few examples of risks that are agency-specific. The agency's name and related objective are included, so that the relationship between the objective and risk can be observed. It is important that you "think outside the box" in order to generate a broad list of risks for your agency. Although some risks will be common to several agencies, there will be several risks that will only be applicable to your agency.

Agency: Arkansas Department of Human Services

Objective: To provide ombudsman services to families involved in the child welfare system to ensure proper treatment.

Risk: Families' rights are abused during the child welfare process.

*This is a very agency-specific risk that would be present on the agency's Division of Children and Family Services tab in the risk assessment.*

(Slide 94)

Agency: Arkansas Department of Correction

Objective: To partner with shelter and rescue organizations to train unwanted dogs inside of institutions and make them more adoptable.

Risk: Inmates and/or staff are injured by an aggressive dog.

Risk: Dogs may become sick or die while in the program.

*These are very agency-specific risk that are only applicable to the agency's Paws in Prison program.*

(Slide 95)

Agency: Arkansas Workers Compensation Commission

Objective: To effectively maintain the law library.

Risk: Publication not added to inventory correctly.

Risk: Publications are lost or stolen.

*These risks are only applicable to agencies that maintain a law library, such as the Workers Compensation Commission.*

(Slide 96)

## Switching gears...

Now that we've discussed what risks are and ways to develop a thorough list of risks, let's switch gears a little, and discuss the appropriate way to rate risks.



(Slide 97)

## Ratings

- The significance or impact and likelihood of each risk should be determined prior to evaluating the control activities that are in place to mitigate the risks.
- A common error when rating risks is to perform the evaluation at the end of the risk assessment process, thus taking existing control activities into consideration.
- It is difficult to “forget” about your control activities when rating the risks, but it is necessary in order to determine accurate ratings. You are rating the **inherent risk**, which is the risk that exists in the absence of internal controls.

(Slide 98)

The significance/impact and likelihood of each risk should be determined prior to evaluating the control activities that are in place to mitigate the risks. A common error when rating risks is to perform the evaluation at the end of the risk assessment process, thus taking existing controls into consideration. It is difficult to “forget” about your controls when you are rating the risks, but it is necessary in order to determine accurate ratings. You are rating the inherent risk; the risk that exists in the absence of internal controls.

Whose responsibility is it to rate risks?



(Slide 99)

It is management's responsibility to rate risks.

## Importance of ratings

The ratings can assist management in making cost-benefit decisions and can help in the design and/or evaluation of control activities.

*(Note: This will be explained in more detail when we discuss control activities.)*



(Slide 100)

It is very important to accurately rate your risks. These ratings can assist management in making cost-benefit decisions and can help in the design and/or evaluation of control activities. This will be explained in more detail when we discuss control activities.

The columns directly to the right of the risks are designated for the ratings. The significance/impact ratings will be placed in the first column, and the likelihood ratings will be placed in the second column.

**Risk Assessment and Control Activities Worksheet**

Agency: \_\_\_\_\_

Department: \_\_\_\_\_

Activity: \_\_\_\_\_

Prepared by: \_\_\_\_\_

Date: \_\_\_\_\_

Objective Type	Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities	Mgmt Conclusion	Corrective Action Plan New or Additional Control Activity
		Risks	Significance / Impact	Likelihood			

(Slide 101)

The columns directly to the right of the risks are designated for the ratings. The significance/impact ratings will be placed in the first column and the likelihood rating will be placed in the second column.

## Significance/Impact

The significance or impact rating signifies the ultimate consequence. How much damage will be done or how much opportunity will be lost if this risk occurs?

- If the answer to this question is, “a lot,” then the risk should be rated **large**.
- If the answer to this question is, “it will cause harm, but there won’t be a significant amount of damage,” rate the risk **moderate**.
- If the answer to this question is, “there won’t be much damage to the agency at all,” rate the risk **small**.

(Slide 102)

The significance or impact rating signifies the ultimate consequence. How much damage will be done or how much opportunity will be lost if this risk occurs? If the answer to that question is, “a lot,” then the risk should be rated “large.” If the risk will cause harm, but there won’t be a significant amount of damage, rate the risk “moderate.” If the risk won’t cause much damage to the agency at all, rate the risk “small.”

## Likelihood

The likelihood rating signifies the likelihood that the risk will occur in the absence of controls. If there are no control activities in place, how probable is it that this risk will occur?

- If the answer to this question is, “very probable,” then the rating should be **high**.
- If the answer to this question is, “it’s possible that the risk may occur, but not definite,” then the rating should be **medium**.
- If the answer to this question is, “the risk is unlikely to occur, even in the absence of controls,” the rating should be **low**.

(Slide 103)

The likelihood rating signifies the likelihood that the risk will occur in the absence of controls. If there are no controls in place, how probable is it that this risk will occur? If the answer to that question is “very probable,” then the rating should be “high”. If it’s possible that the risk may occur, but not definite, then the rating should be “medium.” If the risk is unlikely to occur, even if there are no controls in place, the rating should be “low”.

## Risk Assessment Coordinator

Although rating risks is management's responsibility, it is the responsibility of the risk assessment coordinator to review the ratings before the risk assessment is submitted to DFA Office of Accounting Internal Audit.

If the ratings do not appear to be appropriate, discuss them with management before submitting the risk assessment, and make any changes that are deemed necessary.

(Slide 104)

Although rating risks is management's responsibility, it is the responsibility of the risk assessment coordinator to review the ratings before the risk assessment is submitted to DFA Office of Accounting Internal Audit. If the ratings do not appear to be appropriate, discuss them with management before submitting the risk assessment, and make any changes that are deemed necessary.

## Exercise 2

Rate the following risk:

*An employee is paid for an inaccurate number of hours.*

(Slide 105)

How would you rate the risk that an employee is paid for an inaccurate number of hours?

## Significance/Impact

If this risk occurs, how will it impact the agency? Will it result in a major cash flow problem? Will it make the front page of the newspaper?

**Probably not.**

It would not be good for an employee to be paid for an inaccurate number of hours, but if it happens, it is an easy problem to fix. So, I would probably rate the significance/impact of this risk either **moderate or small**, depending on the size of the agency.

(Slide 106)

If I were rating this risk, I would ask the following questions: If this risk occurs, how will it impact the agency? Will It result in a major cash flow problem? Will it make the front page of the newspaper? Probably not. It would not be good for an employee to be paid for an inaccurate number of hours, but if it happens, it is a pretty simple problem to fix. So, I would probably rate the significance/impact of this risk either moderate or small, depending on the size of the agency.

## Likelihood

In the absence of control activities, how likely is it that an employee could be paid for an inaccurate number of hours? If there is no one verifying the accuracy of the employees' paychecks, is it more likely that errors will be made?

**Yes, very likely.**

I would rate the likelihood of this risk occurring as being **high**.

(Slide 107)

Now, let's look at the likelihood of this risk occurring. In the absence of controls, how likely is it that an employee could be paid for an inaccurate number of hours? If there is no one verifying the hours worked and no one checking the accuracy of the employees' paychecks, is it likely that there will be errors made? I think the answer is yes—very likely. Therefore, I would rate the likelihood of this risk occurring as being high.

## Hint

Before we conclude this section, I would like to give you a few helpful hints.

1. Fraud is NEVER rated low.
2. If EVERY risk in your risk assessment is rated EXACTLY the same way, you will receive a recommendation in your management letter, suggesting that you re-evaluate your ratings.
3. If a risk is rated small and low, you are indicating that it is not necessary to have control activities in place to mitigate the risk.

(Slide 108)

Before we conclude this section, I'd like to give you a few helpful hints.

1. Fraud is NEVER rated low.
2. If EVERY risk in the risk assessment is rated EXACTLY the same way, you will receive a recommendation in your management letter, suggesting that you re-evaluate your ratings.
3. Realize that if a risk is rated small AND low that you are indicating that it is not necessary to have control activities in place to mitigate the risk.

# Questions?



(Slide 109)

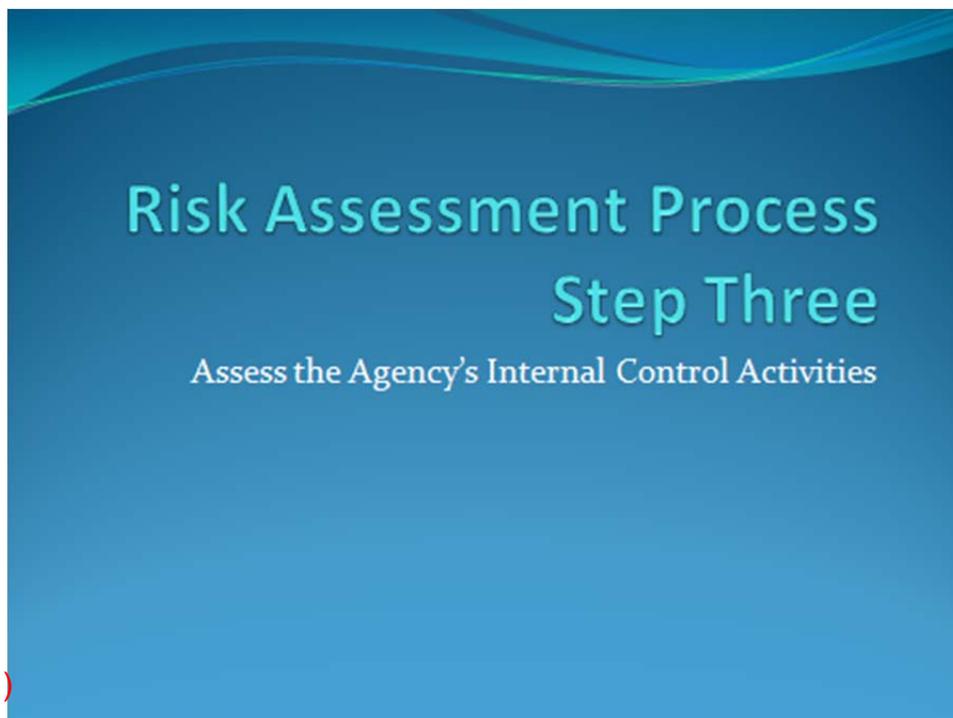
***In conclusion, please remember:***

- A risk is anything that may prevent the agency from meeting its objectives.
- Risks should be identified for each objective.
- Risks should be identified without taking the existing internal controls into consideration.
- The significance/impact and likelihood of each risk should be rated after the risk has been identified.
- All risks should be rated without taking the existing internal controls into consideration.



(Slide 110)

The next step in the risk assessment process is the identification of control activities that will mitigate the risks that have been identified.



(Slide 111)

## CONTROL ACTIVITIES



(Slide 112)

We have identified our objectives and assessed our risks. Now we will discuss the identification and evaluation of control activities.

## Organization first!!!

- The risk assessment workbook has been organized, and objectives and risks have been included for each activity.
- There is a column on the risk assessment spreadsheet entitled, “Actions to Manage Risks/Control Activities.” All of the control activities that are in place to mitigate each risk will be noted in this column.
- If there is more than one control activity in place to mitigate a risk, simply insert additional lines and add the additional control activities.

(Slide 113)

The risk assessment workbook has been organized, and objectives and risks have been included for each activity. There is a column on the risk assessment spreadsheet entitled, “Actions to Manage Risks/Control Activities”. All of the control activities that are in place to mitigate each risk will be noted in this column. If there is more than one control activity in place to mitigate a risk, simply insert additional lines and add the additional control activities.

Risk Assessment and Control Activities Worksheet					
Agency: <u>Arkansas State Board of Massage Therapy</u>		Prepared By: <u>Preparer's Name</u>			
Department: <u>Administration</u>		Date Prepared: <u>Date Reported</u>			
Activity: <u>Payroll/Human Resources</u>					
Objective Type	Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities
		Risks	Significance / Impact	Likelihood	
	Accurate and timely processing of payroll.	Employee is paid for inaccurate number of hours.	Moderate	High	Direct supervisor reviews employee's timesheet and/or leave slips for accuracy and approves by signing and dating.  Separation of duties exists in AASIS between time entry and time approval. Time approver compares data entry to physical time sheet to verify accuracy and ensures proper supervisory signature is present on time sheet.
		Employee uses leave that is not earned.	Moderate	Medium	AASIS controls prevent the posting of leave time that exceeds the available leave balance. A quota balance reconciliation is performed to ensure that the correct number of hours are being added each month based on the appropriate hire date and that extra hours are not being manually added in error.

(Slide 114)

This slide lists two different risks. The first risk has two control activities listed, and the second risk has one control activity. It is easy to determine which controls are related to each risk.

## What are control activities?

COSO defines control activities as the actions established through policies and procedures that help ensure 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.

(Slide 115)

COSO defines control activities as the actions established through policies and procedures that help ensure 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.

## In other words...

- Control activities are the things that are done to help you meet your objectives.
- They accomplish this by helping to mitigate the risks that might prevent the agency from meeting its objectives.

(Slide 116)

In other words, control activities are the things that are done to help meet your objectives. They accomplish this by helping to mitigate the risks that might prevent the agency from meeting its objectives.



## How are control activities identified?

- It's not possible to evaluate internal controls without first identifying the risks that could prevent the agency from meeting its objectives.
- Control activities are directly linked to risks, so begin by reviewing the risks that have been identified.
- Think about everything that is done in order to prevent that risk from being realized.

(Slide 117)

It's not possible to evaluate internal controls without first identifying the risks that could prevent the agency from meeting its objectives. Controls are directly linked to risks, so begin by reviewing the risks that have been identified. Think about everything that is done in order to prevent that risk from being realized.

## Controls by Type

It may be helpful to think of control activities by **type**.

There are two different types of control activities:

- Preventive
- Detective

(Slide 118)

It may be helpful to think of the controls by type.

There are two different types of control activities: preventive and detective.



## Preventive Control Activity

Preventive controls attempt to prevent the risks from occurring.

Example:

- Requirement to receive approval before making purchases.
  - Prevents unauthorized purchases from being made

(Slide 119)

Preventive controls attempt to prevent the risks from occurring. An example of a preventive control is the requirement to receive approval before making purchases. This control will prevent unauthorized purchases from being made.

## Detective Control Activity

Detective controls will detect if the risk occurs. If the risk cannot be prevented, there should be a control activity in place to detect that it has occurred.

Example:

- Reconciliations
  - Bank account reconciliations occur after the period has ended. This will not prevent errors, but will enable the error to be detected and corrected.

(Slide 120)

Detective controls will detect if the risk occurs. If you cannot prevent the risk from occurring, you will need to be able to detect that it has occurred so that you can take the appropriate measures to rectify the problem. An example of a detective control is a reconciliation. Bank account reconciliations occur after the period has ended. They won't prevent errors from occurring, but they will enable you to detect the errors that occurred during the period that is being reconciled. Once you detect the errors, you will be able to fix them.



## Tip

As you are looking at the risk, think about the controls that are in place by type. For example, ask yourself the following questions:

- What do we do to **prevent** this risk from occurring?
- What do we do to **detect** if this risk has occurred?

(Slide 121)

As you are looking at the risk, think about the controls that are in place by type. For example, ask yourself the following questions:

1. What do we do to **prevent** this risk from occurring?
2. What do we do to **detect** if this risk has occurred?

# AGA Fraud Prevention Toolkit

The AGA Fraud Prevention Toolkit is a helpful tool that can be used when evaluating control activities.



(Slide 122)

The AGA Fraud Prevention Toolkit is a helpful tool that can be used when evaluating control activities. I introduced you to the toolkit earlier, when we were discussing the identification of risks. I'd like to show you another aspect of the toolkit now.



## Flashback...

- When we were discussing the identification of risks, I pointed out that the tools in the toolkit can be accessed by business process, program area, or fraud type.
- Under each of these tabs, there is a link to the “tools/best practices” section.
- In this section, you can review information about controls and control environment, risk modeling and risk assessment, master risk tables, data analytics, and an internal controls library.

(Slide 123)

When we were discussing the identification of risks, I pointed out that the tools in the toolkit can be accessed by business process, program area, or fraud type. Under each of these tabs, there is a link to the “tools/best practices” section. In this section, you can review information about controls and control environment, risk modeling and risk assessment, master risk tables, data analytics, and an internal controls library.



## Controls & Control Environment Section

- The controls and control environment section defines internal controls and explains their importance.
- It stresses the importance of maintaining an ethical tone at the top.
- An overview of the COSO framework is provided, and links to each section of the National Association of State Comptrollers (NASC)'s Multi-State Consortium on Internal Control are provided.
- The NASC tool was developed in 2006. The group believed that it would be helpful if states had a web-based internal control tool that was easy to use and would help them to gain a better understanding of the value of internal controls.

(Slide 124)

The controls and control environment section defines internal controls and explains their importance. It stresses the importance of maintaining an ethical tone at the top. An overview of the COSO framework is provided, and links to each section of the National Association of State Comptrollers (NASC)'s Multi-State Consortium on Internal Control are provided. The NASC tool was developed in 2006. The group believed that it would be helpful if states had a web-based internal control tool that was easy to use and would help them to gain a better understanding of the value of internal controls.



There are tools available for each of the following areas:

- Accounting system
- Budgets and planning
- Buy America Act
- Capital Assets Control
- Cash
- Civil Rights and Drug-Free Workplace
- Control Environment
- Davis-Bacon Act
- Federal Student Financial Aid
- Grant Administration Guidance
- Information Systems and Technology
- Investments
- Payables
- Personnel and Payroll
- Receivables
- Risk Assessment

(Slide 125)

There are tools available for each of the following areas:

- Accounting system
- Budgets and planning
- Buy America Act
- Capital Assets Control
- Cash
- Civil Rights and Drug-Free Workplace
- Control Environment
- Davis-Bacon Act
- Federal Student Financial Aid
- Grant Administration Guidance
- Information Systems and Technology
- Investments
- Payables
- Personnel and Payroll
- Receivables
- Risk Assessment

# Example: Personnel and Payroll Section

**Personnel/Payroll**

In public agencies, it is the responsibility of management to ensure that the most effective and efficient use possible is made of the personnel resources available. This responsibility is shared by all levels of management and is essential to the success of the agency.

The document sets out the various responsibilities that apply to the personnel and payroll sections of the agency. It is the responsibility of management to ensure that the personnel and payroll sections are organized and operated in a manner that is consistent with the overall objectives of the agency.

- 1. The personnel and payroll sections are responsible for recruiting, hiring, promotion, discipline and dismissal of all personnel and for maintaining the personnel files, and for maintaining the payroll records.
- 2. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 3. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 4. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 5. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 6. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 7. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 8. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 9. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 10. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.

**Responsibilities of the Personnel and Payroll Sections**

The personnel and payroll sections are responsible for maintaining the personnel and payroll records. This responsibility is shared by all levels of management and is essential to the success of the agency.

- 1. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 2. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 3. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 4. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 5. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 6. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 7. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 8. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 9. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 10. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.

Page 1 of 1

**Personnel/Payroll**

- 1. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 2. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 3. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 4. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 5. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 6. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 7. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 8. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 9. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.
- 10. The personnel and payroll sections are responsible for maintaining the personnel and payroll records.

**Example Organization of the Personnel and Payroll Sections**

Section	Personnel	Payroll	Other	Total
1. Recruitment and hiring				
2. Personnel files and payroll records				
3. Personnel and payroll records				
4. Personnel and payroll records				
5. Personnel and payroll records				
6. Personnel and payroll records				
7. Personnel and payroll records				
8. Personnel and payroll records				
9. Personnel and payroll records				
10. Personnel and payroll records				

Page 2 of 1

(Slide 126)

Let's take a look at the tool for the personnel and payroll section, since this is an area that applies to every agency. We're only going to look at the first few pages of the document, but I think this will provide you with a good understanding of the way the tools are set up.

It is difficult to read the information that is on this slide, but the following slides include highlights of the information that is provided.



The first page begins with the following statement:

*As public servants, it is our responsibility to safeguard taxpayers' dollars in the most effective and efficient way possible while adhering to laws and regulations governing those processes. Internal controls are placed at various points in these processes to ensure that guidelines are followed and that there is accountability to the taxpayers.*

(Slide 127)

The first page begins with the following statement:

As public servants, it is our responsibility to safeguard taxpayer's dollars in the most effective and efficient way possible while adhering to laws and regulations governing those processes. Internal controls are placed at various points in these processes to ensure that guidelines are followed and that there is accountability to the taxpayers.



Then, the document begins to discuss important things to think about when evaluating control activities for this area. Some of the items listed are:

- The agency's policies and procedures for recruiting, training, evaluation, discipline and payroll are in accordance with applicable state and federal laws, rules and collective bargaining agreements.
- Appropriate standards of conduct are communicated and enforced throughout the agency.
- Time worked is accurately recorded and approved.
- Overtime is authorized.
- Payroll is processed timely and accurately.

It's important to ensure that there are control activities in place that will ensure that these things are happening.

(Slide 128)

Then, the document begins to discuss important things to think about when evaluating control activities for this area. Some of the items listed are:

- The agency's policies and procedures for recruiting, training, evaluation, discipline and payroll are in accordance with applicable state and federal laws, rules and collective bargaining agreements.
- Appropriate standards of conduct are communicated and enforced throughout the agency.
- Time worked is accurately recorded and approved.
- Overtime is authorized.
- Payroll is processed timely and accurately.

It's important to ensure that there are control activities in place that will ensure that these things are happening.

## Other information provided

- The document also discusses the importance of segregation of duties and provides examples of the functions that should be segregated.
- There are questionnaires available that will help you to think through each part of the payroll process, to ensure that there are proper control activities in place.
- You can modify the questionnaires so that they will be applicable to your agency.

(Slide 129)

The document also discusses the importance of segregation of duties and provides examples of the functions that should be segregated.

Then, there are questionnaires available that will help you to think through each part of the payroll process, to ensure that there are proper control activities in place. You can take these questionnaires and modify them so that they'll be applicable for your agency. They are all Microsoft Word documents.

B.	Time and Attendance Records:	Yes	No	N/A	Comments
1.	Are all employees required to sign/log in and record daily hours worked and leave time taken?				
2.	Are employees' time and attendance records approved by their supervisors?				
3.	Are time sheets/attendance records checked for computations of the reported pay period hours?				
4.	Is overtime pre-approved and within budgeted amounts?				
5.	If a time clock is used, is it placed where a supervisor can observe it?				
6.	Are time cards used only by the employees to whom they are issued?				
7.	Is leave time pre-approved where appropriate (vacation, compensatory, medical, family, etc.)?				
8.	Are attendance records reviewed by management for excessive absences or tardiness?				
9.	Are appropriate "management of effort" records maintained for payroll charged to federal grants (per OMB Circular A-87)?				
10.	Are procedures established for inputting time and attendance into the payroll system?				
11.	Do procedures exist to review time records for completeness, accuracy and supervisor approval?				
12.	Are corrections to recorded time approved by the employee's supervisor and authorized by management?				

(Slide 130)

This is an example of one of the questionnaires that is available in this toolkit. This questionnaire is for the time and attendance record section of the payroll activity.

If you were using this questionnaire in your brainstorming session, you would go down the list and determine if any of the control activities are currently in place. For example:

1. Are all employees required to sign/log in and record daily hours worked and leave time taken?

If the answer is "yes", then you can include this control activity in your risk assessment. If the answer is "no", then you may need to discuss it in order to determine if this is a control that needs to be implemented. For example, if your employees are **not** required to log their time on timesheets or complete leave request forms, have a discussion with management to determine if this is a control activity that needs to be implemented.

A similar discussion would be held regarding every question to which the answer was "no". Each "yes" response indicates a control activity that is currently in place and should be addressed in the risk assessment.

## Example

Activity: Payroll

Objective: To ensure that payroll is processed accurately and timely.

Risk: Employee is paid for inaccurate number of hours.

The objective and risk will be reviewed first, because we cannot identify control activities until we have first identified the objective and risk.

(Slide 131)

Let's look at an example of control activities for the payroll activity. The objective and risk will be reviewed first, because we cannot identify control activities until we have first identified the objective and risk.

Activity: Payroll  
Objective: Accurate and timely processing of payroll.  
Risk: Employee is paid for inaccurate number of hours.

Controls: Direct supervisor reviews employee's timesheet and/or leave slips for accuracy and approves by signing and dating.

Separation of duties exists in AASIS between time entry and time approval. Time approver compares data entry to physical time sheet to verify accuracy and ensures proper supervisory signature is present on time sheet.

(Slide 132)

What types of control activities are present?

### **Preventive**

The employee's supervisor must review and sign the timesheets and leave slips before they are processed. The time approver compares the data entry to the physical time sheet to verify accuracy. All of this is done prior to the timesheets and leave slips being processed, in order to prevent errors from occurring.

(Slide 133)

## Quiz—Question 1

**What are examples of additional preventive control activities that could help to mitigate this risk?**

Activity:	Payroll
Objective:	Accurate and timely processing of payroll.
Risk:	Employee is paid for inaccurate number of hours.
Controls:	Direct supervisor reviews employee's timesheet and/or leave slips for accuracy and approves by signing and dating. Separation of duties exists in AASIS between time entry and time approval. Time approver compares data entry to physical time sheet to verify accuracy and ensures proper supervisory signature is present on time sheet.

(Slide 134)

What are some examples of additional preventive control activities that could mitigate the risk of an employee being paid for an inaccurate number of hours?

## Additional Preventive Controls

Activity: Payroll  
Objective: Accurate and timely processing of payroll.  
Risk: Employee is paid for inaccurate number of hours.

- Employees receive job training (including AASIS training) when hired and updated training as needed. Staff meetings are held to keep employees informed.
- Clear and concise written policies and procedures exist for the payroll process. Policies are kept current.
- There are clear and open lines of communication, and employees are encouraged to seek advice as needed.

(Slide 135)

The following are a few examples of additional preventive control activities that could mitigate the risk of an employee being paid for an inaccurate number of hours:

- Employees receive job training (including AASIS training) when hired and updated training as needed. Staff meetings are held to keep employees informed.
- Clear and concise written policies and procedures exist for the payroll process. Policies are kept current.
- There are clear and open lines of communication, and employees are encouraged to seek advice as needed.

## Quiz—Question 2

**What are examples of detective control activities that could help to mitigate this risk?**

Activity:	Payroll
Objective:	Accurate and timely processing of payroll.
Risk:	Employee is paid for inaccurate number of hours.
Controls:	Direct supervisor reviews employee's timesheet and/or leave slips for accuracy and approves by signing and dating. Separation of duties exists in AASIS between time entry and time approval. Time approver compares data entry to physical time sheet to verify accuracy and ensures proper supervisory signature is present on time sheet.

(Slide 136)

What are some examples of detective controls that would help to detect if this risk occurred?

## Detective Control Activities

Activity: Payroll  
Objective: Accurate and timely processing of payroll.  
Risk: Employee is paid for inaccurate number of hours.

- Employees review their remuneration statements and are aware of how to report inaccurate pay.
- Management reviews the payroll comparison report in AASIS and investigates any discrepancies. *(large agency)*
- Management reconciles all payroll transactions posted to AASIS to original timesheet/leave requests to ensure accuracy of postings. *(small agency)*

(Slide 137)

The following are a few examples of detective controls that would help to detect if this risk occurred:

- Employees review their remuneration statements and are aware of how to report inaccurate pay.
- Management reviews the payroll comparison report in AASIS and investigates any discrepancies.
- Management reconciles all payroll transactions posted to AASIS to original timesheet/leave requests to ensure accuracy of postings.

## Tips

- Your preventive controls will most likely be encompassed in your policies and procedures. These are the routine steps that you are required to take when performing your daily job duties.
- Required training and written policies and procedures are great preventive controls for almost every activity.
- Management oversight, periodic reconciliations, and review of system-generated reports are great detective controls for almost every activity.
- The DFA Office of Accounting Internal Audit website contains examples of acceptable control activities. Duplicate them in your risk assessment, if the controls are actually being performed.

(Slide 138)

Your preventive controls will most likely be encompassed in your policies and procedures. These are the routine steps that you are required to take when performing your daily job duties. Required training and written policies and procedures are great preventive controls for almost every activity.

Management oversight, periodic reconciliations, and review of system-generated reports are great detective controls for almost every activity.

If there are control activities listed on one of the risk assessment examples that have been provided on the DFA Office of Accounting Internal Audit website, please feel free to duplicate the wording for these controls, as long as the control activities are actually being performed.

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

## Include Position Titles

It is important to include position titles within the control activities.

Example:

- Instead of simply stating that a report is reviewed each month, include the title of the individual who is reviewing the report.
- Enables anyone who reviews the risk assessment document to clearly tell who is performing the control.

(Slide 139)

One thing that I would like to point out about control activities is the importance of including position titles. For example, rather than simply stating that a report is reviewed each month, include the title of the individual who is reviewing the report. This will enable anyone who reviews the risk assessment document to clearly tell who is performing the control activity.

If there is more than one individual responsible for performing a particular control activity and they have the same title, put numbers behind the title. This will enable anyone who is reviewing the document to tell that there are different people responsible for the different tasks. For example, you may state that Administrative Analyst #1 does one activity and Administrative Analyst #2 does another activity.

- Objectives



- Risks



- Controls



- Ratings



(Slide 140)

The agency's objectives have been identified, risks have been identified for each objective, and control activities have been identified for each risk. Now it is time to discuss the proper way to evaluate, or "rate", the control activities.

## Rating Controls

The risk assessment workbook has been organized, objectives and risks have been included for each activity, control activities have been identified for each risk.

- **Management** should review the control activities and determine if they are sufficient.
- Ratings will be listed under the column that is entitled, "Mgmt conclusion."

(Slide 141)

At this point in the process, the risk assessment spreadsheet has been properly organized, the agency's objectives have been identified, risks have been identified for each objective, and control activities have been identified for each risk. Now it is management's responsibility to ensure that the control activities that have been identified are sufficient.

**Risk Assessment and Control Activities Worksheet**

Agency: \_\_\_\_\_

Department: \_\_\_\_\_ Prepared By: \_\_\_\_\_

Activity: \_\_\_\_\_ Date Prepared: \_\_\_\_\_

Objective Type	Objectives	Risk Assessment			Actions to Manage Risks/ Control Activities	Mgmt Conclusion	Corrective Action Plan New or Additional Control Activity
		Risks	Significance / Impact	Likelihood			



(Slide 142)

There is a column in the risk assessment spreadsheet entitled “Mgmt Conclusion.” The control activities ratings will be placed in this column.

## Rating Controls

If the controls appear to mitigate the stated risk:

- Sufficient
  - Place an “S” in this column

If the controls do not appear to mitigate the stated risk:

- Not Sufficient
  - Place an “NS” in this column

(Slide 143)

Management should review the control activities that have been identified and determine if they are sufficient. If the controls are deemed sufficient, an “S” will be placed in this column. If it does not appear that the controls listed will mitigate the stated risk, an “NS” will be placed in this column, to indicate that the controls listed are not sufficient.

## Misconceptions

The following are a few misconceptions regarding internal control activities:

- The more control activities in place, the better.
- We **MUST** have controls in place to mitigate **EVERY** risk.

(Slide 144)

The following are a few common misconceptions regarding internal controls:

- The more controls in place, the better.
- We **MUST** have controls in place to mitigate **EVERY** risk.

There are some risks that may not need to be as well-controlled as other risks.

## Evaluating Control Activities

- When evaluating control activities, a cost-benefit analysis must be performed.
- The risks have been rated at this point in the process, so we know whether or not the risk is likely to occur and how large an impact it will have on the agency if the risk is realized.
- If there is only a remote chance that the risk will occur, and it wouldn't make a huge difference even if it did occur (so the risk was rated "small and low"), you don't need ten controls in place to mitigate the risk. You may not need any controls at all. Reallocate those resources to other areas, so that you will be better able to mitigate the larger risks.

(Slide 145)

When evaluating internal controls, a cost-benefit analysis must be performed. The risks have been rated at this point in the process, so we know whether or not the risk is likely to occur and how large an impact it will have on the agency if the risk is realized. If there is only a remote chance that the risk will occur, and it wouldn't make a huge difference even if it did occur, you don't need ten controls in place to mitigate the risk. You may not need any controls at all. Reallocate those resources to other areas, so that you will be better able to mitigate the larger risks.

## Evaluating Control Activities

- If your agency has very limited resources, it may be difficult to implement all of the controls that you believe are needed to mitigate a particular risk.
  - In this instance, more management oversight may be necessary.
- Remember, management oversight is a good detective control. You may not be able to prevent the risk from occurring, but you can have controls in place that will allow you to detect that it has occurred.
- Problems will be identified early, if detective controls are in place.

(Slide 146)

If your agency has very limited resources, it may be difficult to implement all of the controls that you believe are needed to mitigate a particular risk. In this instance, more management oversight may be necessary. Remember, management oversight is a good detective control. You may not be able to prevent the risk from occurring, but you can have controls in place that will allow you to detect that it has occurred. Problems will be identified early, if detective controls are in place.



## Corrective Action Plan

If management deems some of the controls to be not sufficient, then a corrective action plan should be developed.

- 1) List additional future control activities
  - Include anticipated implementation date

OR

- 2) State there are no feasible control activities that can be put into place to mitigate the stated risk, and management accepts the possibility that the risk may occur.

(Slide 147)

In a perfect world, there would be sufficient controls in place for every risk that has been identified. Unfortunately, that won't be the case for every agency. If management deems some of the controls to be not sufficient, then a corrective action plan should be developed. The corrective action plan will either:

1. List additional control activities that will be put into place at a future date in order to mitigate the stated risk. The anticipated implementation date will be included as well.

OR

2. State that there are no feasible control activities that can be put into place to mitigate the stated risk, and management accepts the possibility that the risk may occur.

This is a good opportunity for management to determine if process changes are needed or if resources need to be reallocated in order to better serve the agency.

# Questions?



(Slide 148)

Please remember,

- Control activities are the things that are done to help meet your objectives. They accomplish this by helping to mitigate the risks that might prevent the agency from meeting its objectives.
- Preventive controls attempt to prevent the risks from occurring.
- Detective controls will detect if the risk occurs.
- Management is responsible for determining if the control environment is adequate.



(Slide 149)

Next, we will briefly discuss disaster recovery plans and how to implement them into the risk assessment.

Then, there will be a recap of the questions that should have been answered during this workshop.



## Continuity of Operations Plan

If your agency has developed a Continuity of Operations plan, also referred to as a Disaster Recovery plan, you already have a great source that contains the control activities that are in place for your agency's essential processes. Each agency should already have a disaster recovery plan in place that is reviewed by the Division of Legislative Audit when they come out to pay you a visit.

(Slide 150)

If your agency has developed a Continuity of Operations plan, also referred to as a Disaster Recovery plan, you already have a great source that contains the control activities that are in place for your agency's essential processes. Each agency should already have a disaster recovery plan in place that is reviewed by the Division of Legislative Audit when they come out to pay you a visit.

We will provide you an overview of what should be present in your agency's disaster recovery plan.

### FEMA's ELEMENTS OF A VIABLE COOP PLAN

- Essential Processes - What they do on a daily basis for all divisions on the high level.
- Orders of Succession - Primary, secondary, and tertiary person(s) to take over a specific job if the normal person in that position is no longer available.
- Delegations of Authority - Main management positions and the line that is followed if they are needed.
- Interoperable Communications - Having all employee home, work, cell and emergency contact numbers as well as alternate e-mail addresses and vendor contact information.
- Vital Records - Any record (paper or electronic) that is needed to complete a process
- Human Capital - Including all members of an organization and the specific skills/attributes they are capable of doing.
- Alternate locations - Back-up sites, homes, restoration sites, and offsite storage spaces.
- Devolution planning - Who will take responsibility of processes if no one is no longer available to continue them
- Reconstitution - Return to normal operations.

(Slide 151)

FEMA has provided guidance for the development of disaster recovery plans. Each plan should include the following:

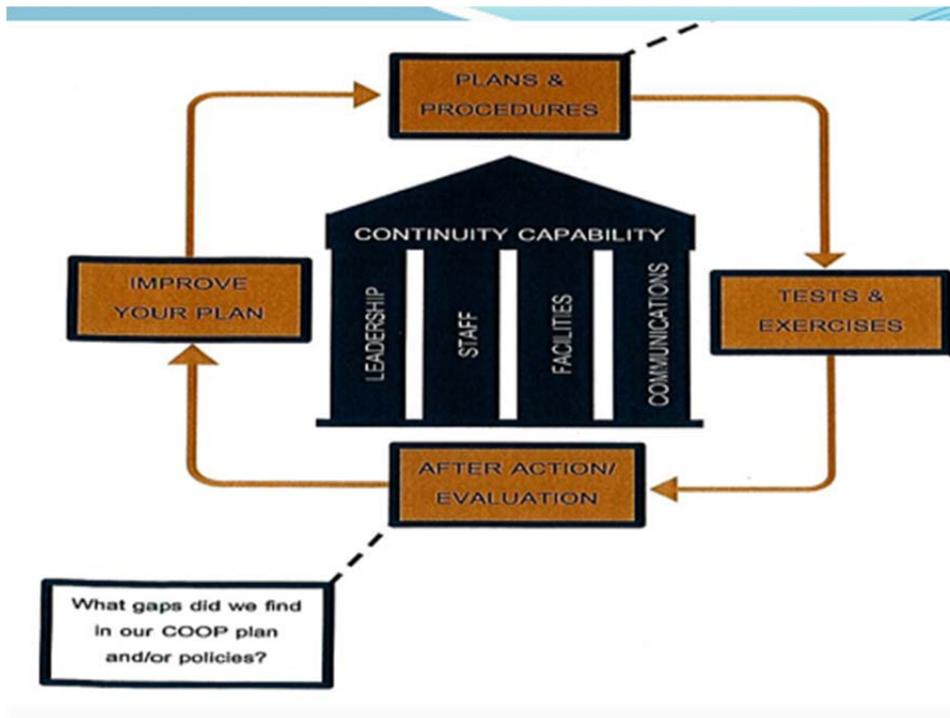
- Essential Processes (what you do on a daily basis for each division)
- Orders of Succession (who will perform the job duties if the responsible person is unable to do so)
- Delegations of Authority (a list of the main management positions and the line that is followed if needed)
- Interoperable Communications (having all employees home, work, cell, and emergency contact information)
- Vital Records (a list of all records that are needed to complete a process)
- Human Capital (a list of all employees and the specific skills they are capable of doing)
- Alternate locations (back up sites, restoration sites, and offsite storage spaces)
- Devolution planning (who will take responsibility of the processes if there is no one who is available to do them)
- Reconstitution (the steps that are necessary to return to normal operations)

## Disaster Recovery Plan Process

1. Develop policies and procedures for your essential processes.
2. Test the plan, to ensure that it is feasible and addresses all potential issues.
3. Evaluate your plan, to determine areas that need to be revised.
4. Make any revisions that are deemed necessary in order to improve the plan.

(Slide 152)

Developing these policies and procedures is the first step in developing a disaster recovery plan. Once you complete your plan, you should test it to ensure that the plan is feasible and addresses all potential issues. Once you complete your testing, you will evaluate your plan. Your tests should have revealed any gaps that exist in your plan. Finally, you will improve your plan. Make any necessary revisions. Develop additional processes and control activities if necessary.



(Slide 153)

This is a visual representation of the information that was included in the previous slide. This is a continuous process.



## Examples of potential disasters

- If every manager in your agency was exposed to a new strain of the flu during a management meeting and all ended up spending a month in the hospital, what would you do? Would the remaining staff be able to keep the agency running?
- If a tornado destroyed your building, what would the agency do in order to ensure that it could continue to function?

(Slide 154)

There are many, many different types of disasters that could occur.

If every manager in your agency was exposed to a new strain of the flu during a management meeting and all ended up spending a month in the hospital, what would you do? Would the remaining staff be able to keep the agency running? Or, if a tornado destroyed your building, what would the agency do in order to ensure that it could continue to function?



## Relation to risk assessment

This plan is an excellent control activity for the risk that an unforeseen disaster occurs. For this reason, the disaster recovery plan should be included as a control activity for the risk that a disaster occurs that affects one of your essential processes.

(Slide 155)

This plan is an excellent control activity for the risk that an unforeseen disaster occurs. For this reason, the disaster recovery plan should be included as a control activity for the risk that a disaster occurs that affects one of your essential processes.

As was previously stated, your agency's disaster recovery plan should include the policies and procedures surrounding your agency's essential processes. These are the processes that the agency **MUST** have in order to function. For example, DFA must be able to run payroll for the state, even in the event of a disaster. The payroll process is an essential function for this agency.

## Relation to risk assessment

The following risk and control activity should be included for each objective that relates to an essential process:

Risk: Disaster occurs.

Control: Management has developed a Continuity of Operations plan that addresses all essential processes. This plan is periodically tested and management ensure it is updated when necessary.

(Slide 156)

The following risk and control activity should be included for each objective that relates to an essential process:

Risk: Disaster occurs.

Control: The agency has developed a Continuity of Operations plan that addresses all essential processes. This plan is periodically tested and is updated when necessary.

Note: Only include this risk and control activity in your risk assessment if the control is actually being performed and tested.

# Questions?



(Slide 157)

Please remember,

- If your agency has developed a Continuity of Operations plan, also referred to as a Disaster Recovery plan, you already have a great source that contains the control activities that are in place for your agency's essential processes.
- This plan is an excellent control activity for the risk that an unforeseen disaster occurs. For this reason, the disaster recovery plan should be included as a control activity for the risk that a disaster occurs that affects one of your essential processes.

## Workshop Recap



(Slide 158)

This workshop was designed to answer nine specific questions. Let's go over those questions one more time, to ensure that everyone has a clear understanding of the answers.

## Goal was to answer the following:

1. What is the Control Self-Assessment approach to risk assessment?
2. What is the role of the risk assessment coordinator?
3. What is an effective and efficient way for an organization to conduct risk assessment?
4. How should risk assessment be documented and organized?
5. What are objectives and how should they be formed?

(Slide 159)

### 1. What is the Control Self-Assessment approach to risk assessment?

When we say taking the control self-assessment approach to agency risk assessment, what we mean is that conducting agency risk assessment should be done through workshops facilitated by agency risk assessment coordinators and management with employees to determine objectives, risks and control activities. After these have been determined then it is management's responsibility to determine if the control activities in place are sufficient.

### 2. What is the role of the risk assessment coordinator?

- The risk assessment coordinator is responsible for overseeing the risk assessment process. This includes the following:
  - Coordinating the brainstorming workshops for the agency
  - Compiling every department's information into a single document
  - Ensuring that management has considered all objectives.
  - Ensuring that management has properly evaluated/rated all risks and control activities.
- Communicating with Internal Audit and submitting the final document.

### 3. What is an effective and efficient way for an organization to conduct risk assessment?

- The risk assessment coordinator should organize brainstorming workshops for management and employees, in order to help identify risks and control activities.
    - These workshops should be organized by objective and should be limited to 5-10 individuals in order to be effective.
  - The risk assessment coordinator should oversee the process; however, each section within the agency should be responsible for completing their portion of the risk assessment.
4. How should risk assessment be documented and organized?
- Risk assessments should be documented on the spreadsheets provided.
  - The agency's name, department, activity, preparer, and date prepared will be listed at the top of each sheet.
  - Each spreadsheet will contain the same columns: objectives, risks, significance/impact, likelihood, control activities, management conclusion, and corrective action plan.
  - Each tab in the risk assessment workbook will contain a different worksheet.
  - The size of the agency will determine the content of the spreadsheets.
    - Large agencies will find it helpful to use a separate tab for each division of the agency.
      - Smaller agencies will find it more appropriate to use a different tab for the actual activities that are performed in the agency.
5. What are objectives and how should they be formed?
- Objectives are the short-term goals that the organization wants to accomplish.
  - They are the pieces that make up the agency's overall goals and mission.
  - There are three different categories of objectives: reporting, operational, and compliance.
  - Objectives should be developed by management.
  - Objectives should be developed for each department within the agency.
  - Objectives often begin with "to ensure", because they reflect a desired outcome.



## Goal was to answer the following:

6. What are risks and how are risks identified and rated?
7. What is the appropriate level of depth when assessing risk?
8. What are control activities and how are control activities determined to be sufficient?
9. When do corrective action plans need to be documented and what should be included?

(Slide 160)

### 6. What are risks, and how are risks identified and rated?

- A risk is anything that may prevent the agency from meeting its objectives.
- In order to thoroughly identify the agency's risks, it is recommended that you conduct a brainstorming session with employees from each level of the organization.
- It is everyone's responsibility to identify risks, but it is management's responsibility to evaluate, or rate, the risks that have been identified.
- The significance or impact rating signifies the ultimate consequence and is indicated by a rating of large, moderate, or small.
- The likelihood rating signifies the likelihood that the risk will occur in the absence of controls and is indicated by a rating of high, medium, or low.
- All risks should be rated without considering the control activities that are in place.

7. What is the appropriate level of depth when assessing risk?

- All risks that may prevent the agency from meeting its objectives should be identified.
- Events can still be risks, even if they are well controlled. Do not eliminate potential risks, simply because there are control activities in place.
- Think outside the box. If management later determines that risks are not relevant, they can be removed at that time.

8. What are control activities, and how are control activities determined to be sufficient?

- Control activities are the things that are done to help meet your objectives. They accomplish this by helping to mitigate the risks that might prevent the agency from meeting its objectives.
- Preventive controls attempt to prevent the risks from occurring.
- Detective controls will detect if the risk occurs.
- Management is responsible for determining if the control environment is adequate.

9. When do corrective action plans need to be documented, and what should be included?

If management deems some of the controls to be not sufficient, then a corrective action plan should be developed. The corrective action plan will either:

3. List additional control activities that will be put into place at a future date in order to mitigate the stated risk. The anticipated implementation date will be included as well.

OR

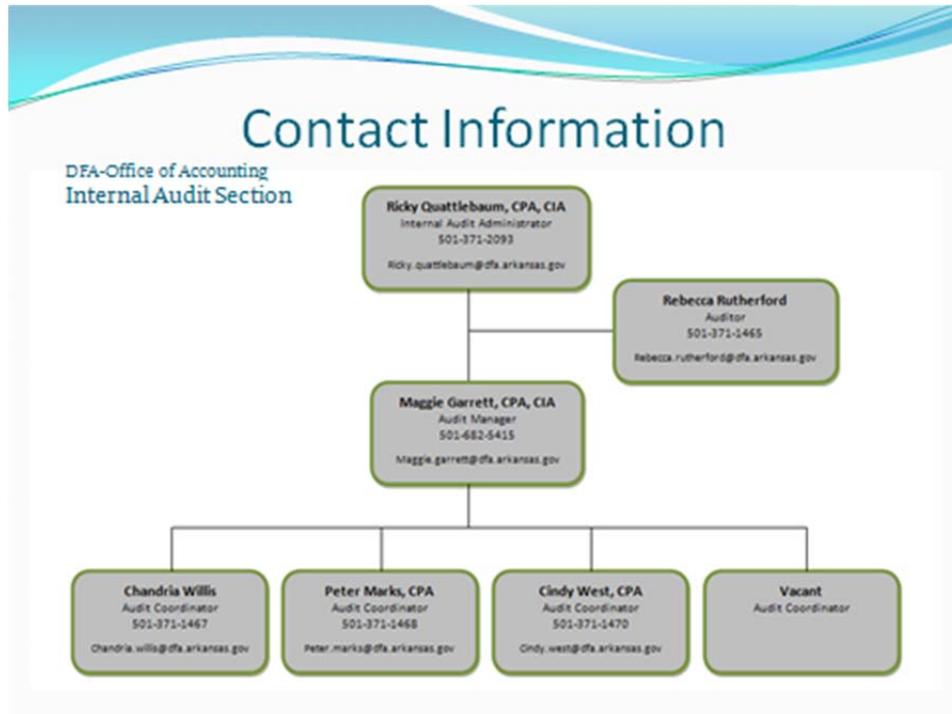
4. State that there are no feasible control activities that can be put into place to mitigate the stated risk, and management accepts the possibility that the risk may occur.

# Questions?



(Slide 161)

If you have any questions about any of the areas that have been discussed, please do not hesitate to contact someone in our office. The contact information is presented on the following slide.



(Slide 162)



(Slide 163)