



Internal Audit Risk Assessment and Audit Planning

May 6, 2011

Eric Miles, Partner, CPA, CIA, CFE

Ric Jazaie, CPA, CIA

MOSS ADAMS_{LLP}

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.



Today's Objectives

- Provide an overview of current internal audit planning and risk assessment practices
- Review internal audit planning and risk assessment benchmark data
- Compare current California community college internal audit planning and risk assessment practices
- Discuss common internal audit planning and risk assessment pitfalls



Detailed Agenda

- Background
- Risk Assessment and Audit Planning Process
 - Identify Risks
 - Sketch Audit Universe
 - Define Objectives Universe
 - Develop Risk Universe
 - Validate Audit Universe
 - Measure Risks
 - Determine Factors
 - Weight Risk Factors
 - Score Risk Factors
 - Prioritize Risks and Select Audits
- Summary
- Q&A



Disclaimer

The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.



Source Material

- Assessing Risk (2nd Edition), David McNamee, IIA Research Foundation 2004
- Brink's Modern Internal Auditing (7th Edition), John Wiley & Sons, 2009
- Sawyer's Internal Auditing (5th Edition), IIA 2005



Risk Assessment and Audit Planning

- Risk: The possibility of an event occurring that will have an impact on the achievement of objectives.
- Risk Assessment: the consideration of the probable material effects of uncertain events. It is the identification, measurement, and prioritization of risks and auditable areas. Further, it allows the auditor to design more specific and effective audit programs.

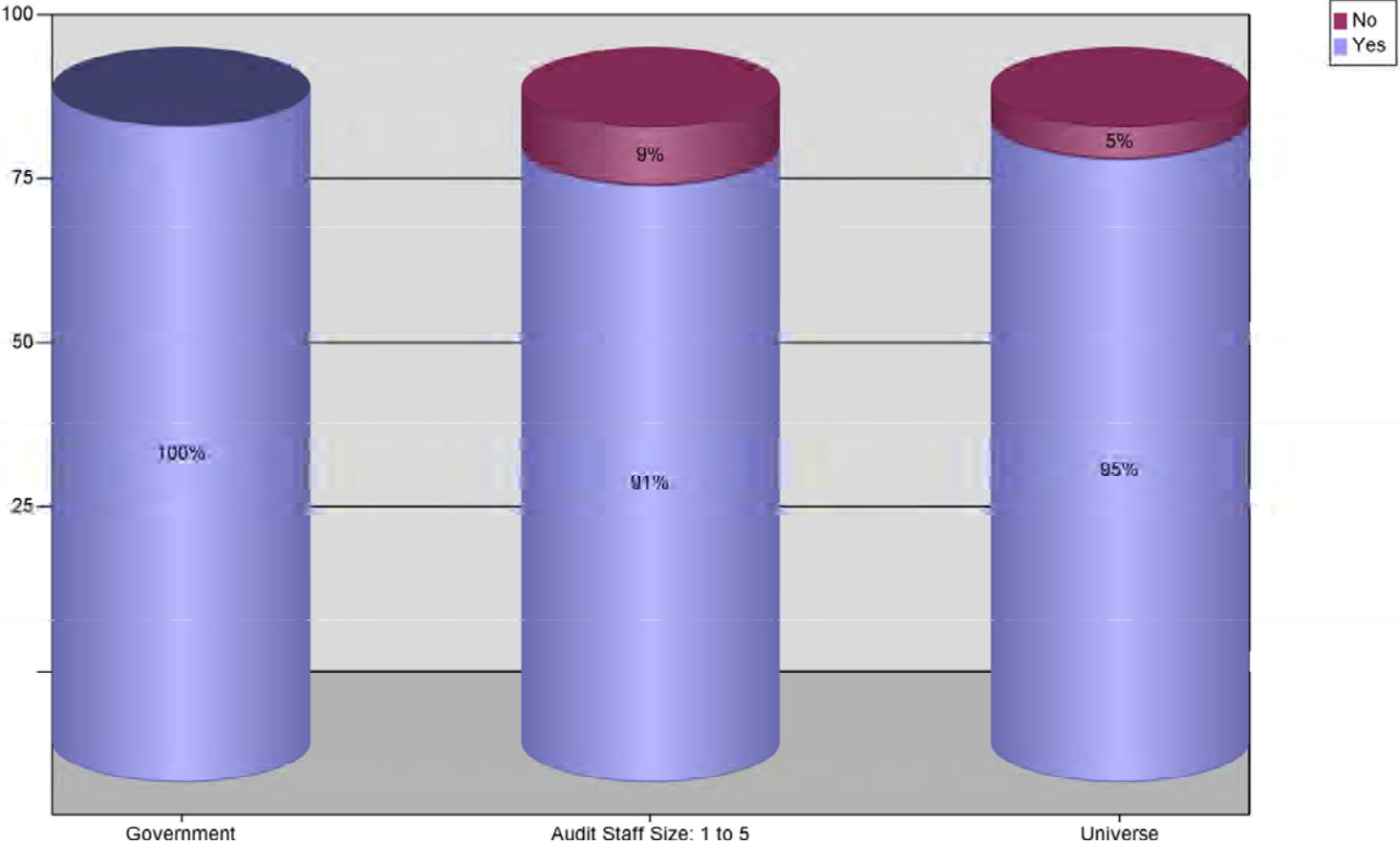
Do you use a formal risk assessment process for internal audit planning?

1. Yes
2. No



Use of Risk Assessment in Internal Audit

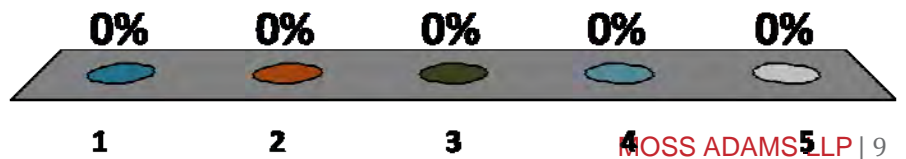
Presence of Formal Risk Assessment Process for Internal Audit



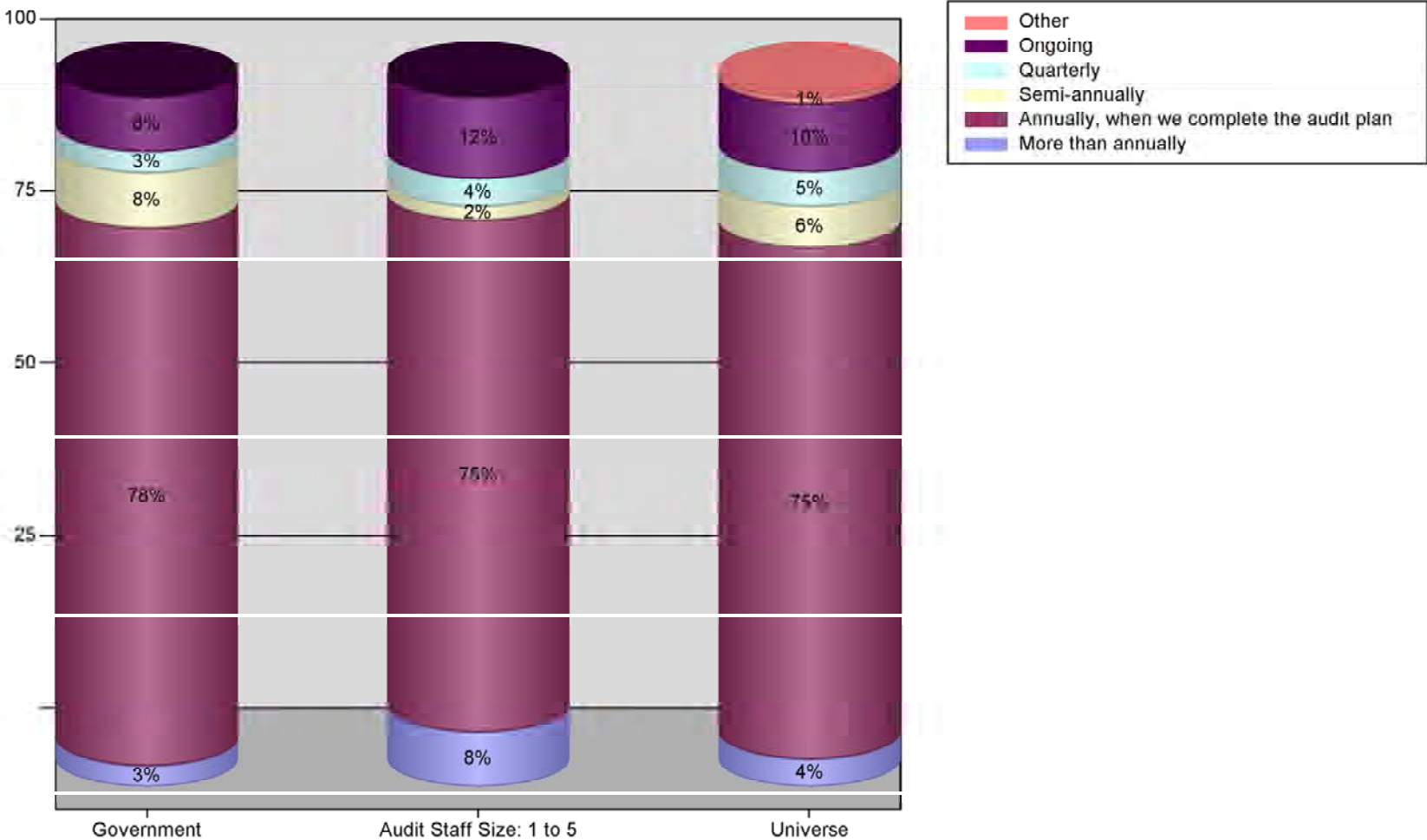
Source: IIA GAIN 2009 Benchmark Study

How often do you perform an Internal Audit Risk Assessment?

1. Bi-annually +
2. Annually
3. Semi-annually
4. Quarterly
5. Other/We don't



Frequency of Internal Audit Risk Assessments



Source: IIA GAIN 2009 Benchmark Study

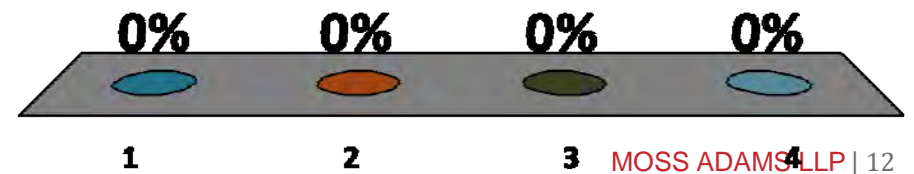


Why Risk-Based Audit Planning?

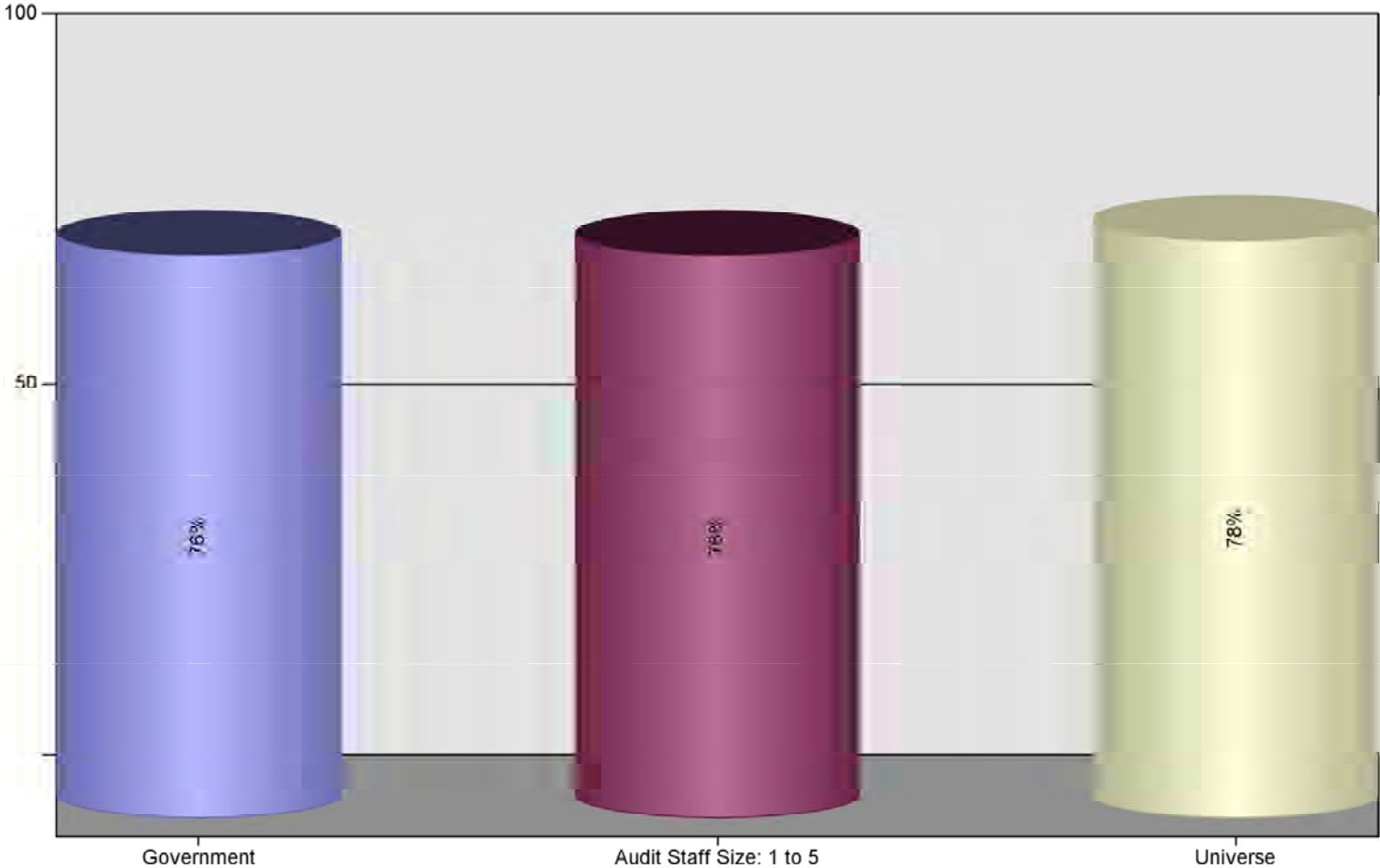
- IPPF Performance Standard 2010.A1 – “The internal audit activity’s plan of engagements must be based on a **documented risk assessment, undertaken at least annually**. The input of the senior management and the board must be considered in this process.”
- More than a requirement
 - Makes the best use of limited resources
 - Improves ability to impact organization
 - Generates buy-in from management
 - Creates **value**

What percentage of your audit recommendations are implemented by Management?

1. 75% - 100%
2. 50% - 75%
3. 25% - 50%
4. 0% - 25%



Percent of Recommendations Implemented



Source: IIA GAIN 2009 Benchmark Study



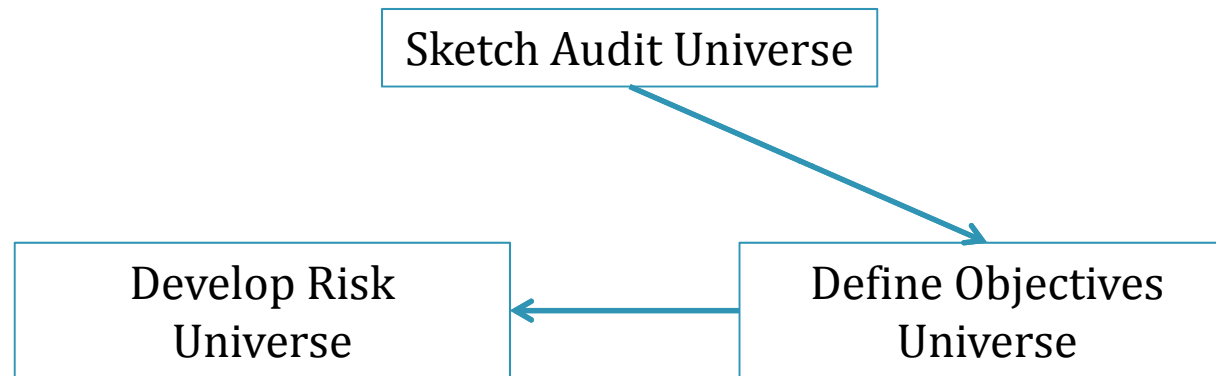
What Makes Risk-Based Audit Planning Difficult?

- Lack of understanding of risk concepts
- Lack of specialized knowledge (e.g. IT)
- No time to plan (the continuous “do” loop)
- Lack of senior management and Board support (i.e. strict compliance)
- Perceived lack of impact on value perception (i.e. it wouldn’t make a difference)
- Paralysis through analysis

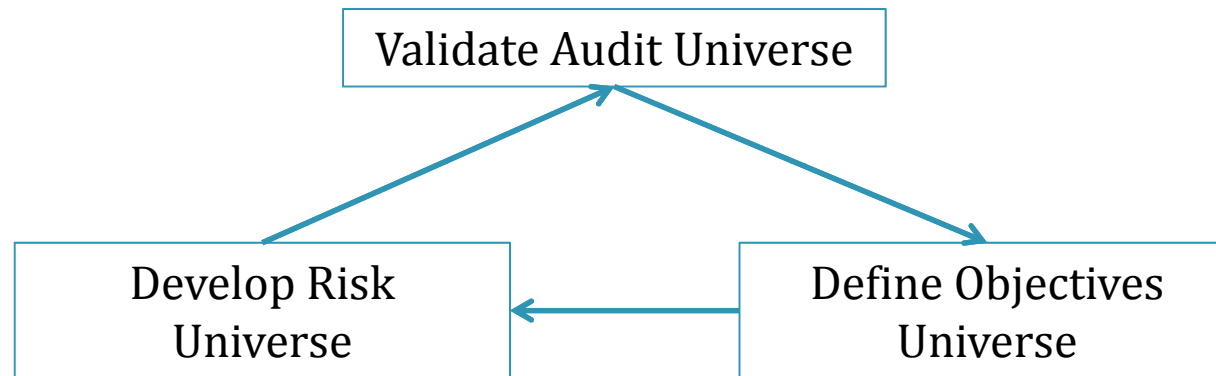
Risk Assessment Process Overview



Identify Risks



Identify Risks





Identify Risks

Sketch Audit Universe



Identify Risks

- “Sketch” the Audit Universe
 - Audit Universe – The sum of all auditable units.
 - Auditable Unit – Parts of the organization that are exposed to sufficient risks that control, including audit, is appropriate.
 - The “sketch” frames risk identification (i.e. who IA talks to, what info is gathered and how risk is identified).
 - The initial audit universe need not be complete but should be verified and completed through the risk assessment process.
 - Types of units: projects, IT systems, business functions, departments, business processes/sub-processes, assets (physical, financial, human,intangible)

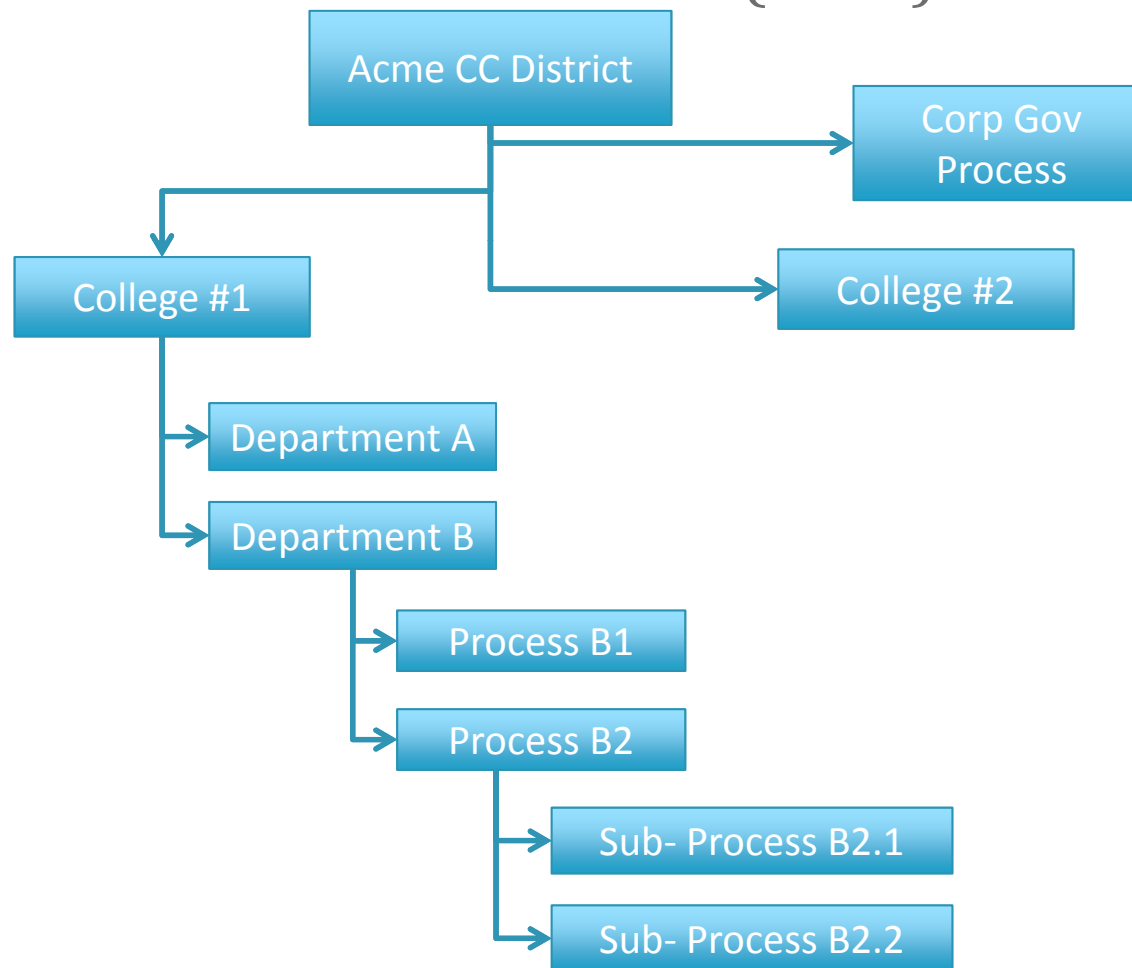


Identify Risks

- “Sketch” the Audit Universe (cont.)
 - Categories of Auditable Units: projects, IT systems, business functions, departments, business processes/sub-processes, assets (physical, financial, human, intangible)
 - Criteria for selecting Auditable Units:
 - Contribute to the organizations goals.
 - Are sufficiently large as to have a noticeable impact on the organization
 - Are sufficiently important to justify the cost of control
 - Minimize the categories of auditable units when possible.

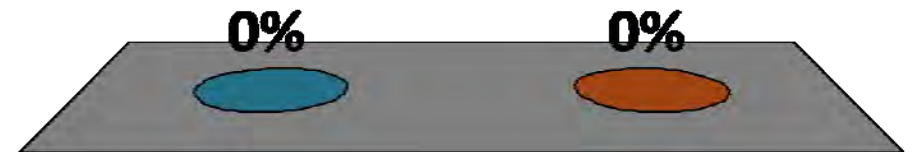
Identify Risks

- “Sketch” the Audit Universe (cont.)

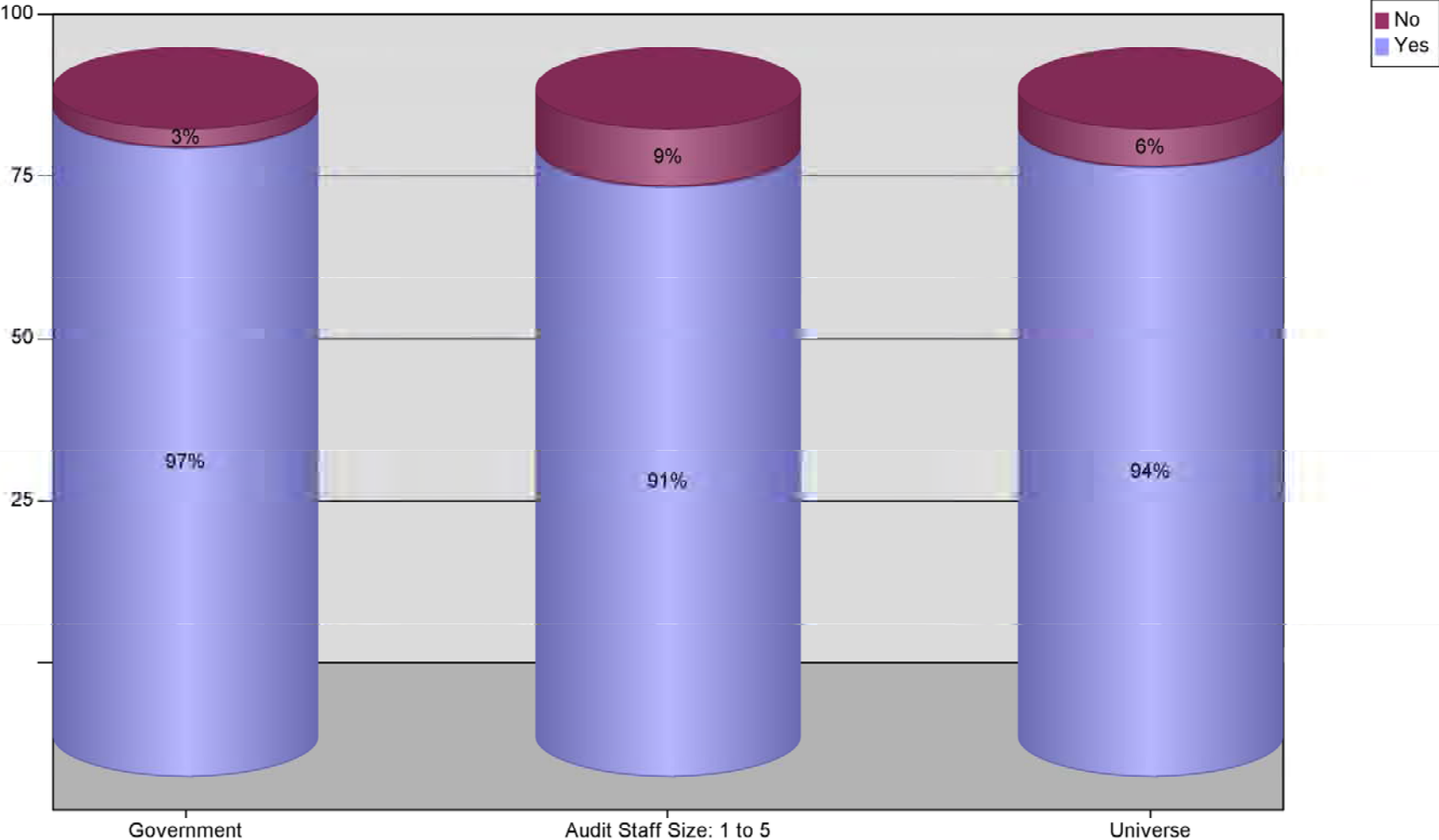


Do you have a formally documented Audit Universe?

1. Yes
2. No



Formally Documented Audit Universe



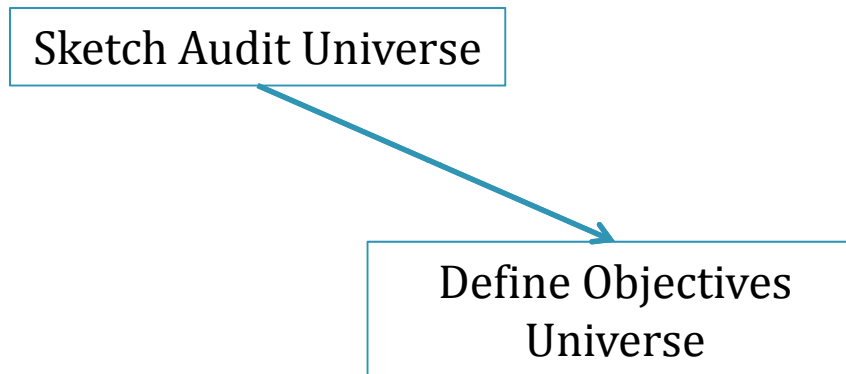
Source: IIA GAIN 2009 Benchmark Study

Audit Universe Categorization

Category	Government	Audit Staff: 1 to 5	Universe
Departments	97%	89%	86%
Processes	97%	89%	93%
Service Line	58%	40%	55%
Organization Units/Locations	81%	61%	78%
Programs	75%	33%	51%
ERM Risk Portfolio	28%	30%	34%
Other	22%	14%	17%

Source: IIA GAIN 2009 Benchmark Study

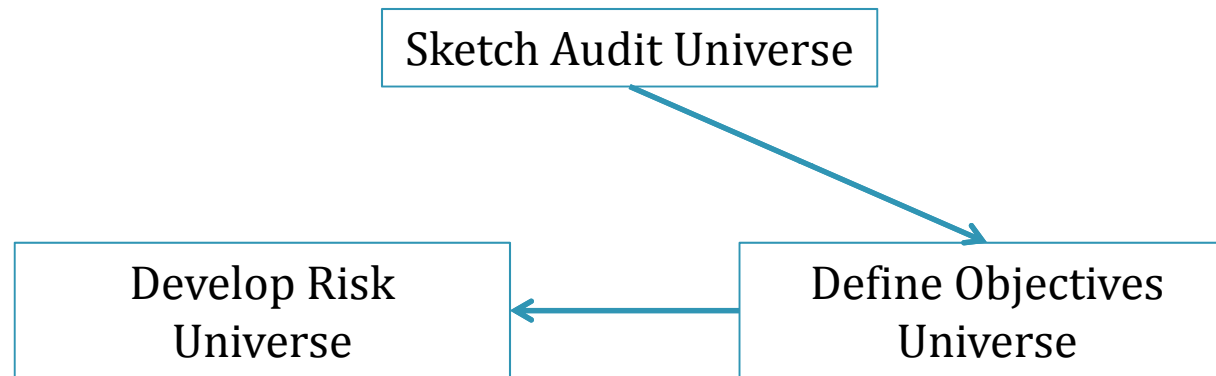
Identify Risks



Identify Risks

- Define the “Objectives Universe”
 - Objectives Universe: I made this one up. Key objectives for each Auditable Unit
 - Risks only exists in the context of the achievement of an objective...if you don't know the objective you can't identify the risk.
 - Categories of objectives
 - Reliability and integrity of financial and operational information
 - Effectiveness and efficiency of operations.
 - Safeguarding of assets.
 - Compliance with laws, regulations, and contracts.

Identify Risks



Identify Risks

- Develop the “Risk Universe”
 - Arguably the **most important step** in the entire process. Everything else follows the identification of risk. If you don’t identify it you can’t measure, prioritize or manage.
 - Requirements for successful risk identification:
 - Thorough understanding of operations of Auditable Units
 - A process through which to generate a reasonable list of possible risks. Common methods include a combined use of:
 - Risk framework (see below)
 - Management questionnaires
 - Management interviews

Identify Risks

- Develop the “Risk Universe” (Cont.)
 - Analogies to similar operations
 - Prior audit results
 - Industry surveys and benchmarking
 - Other research
- Use of a Risk Framework
 - Exposure Analysis: Risk from the perspective of the primary assets of the organization, including all four types of assets (physical, financial, human, and intangible). Primarily areas with significant reliance on capital equipment.



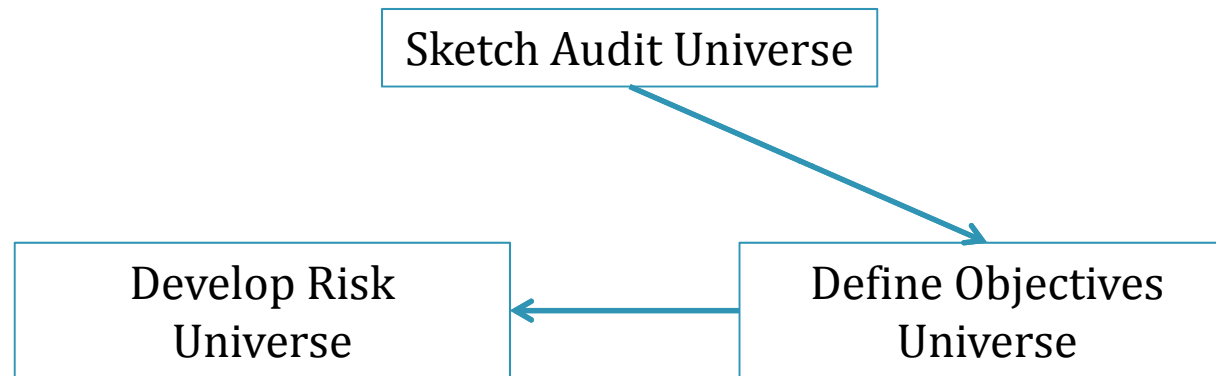
Identify Risks

- Develop the “Risk Universe” (Cont.)
 - Environmental Analysis: Risk from the perspective of changes to the external environments and their effects on management processes and controls. Environmental analysis works best in service-oriented processes and those that are highly regulated or competitive, although nearly every auditable unit is affected by environmental risk to some extent. Areas of environmental risk include:
 - Physical environment: Site, location, weather, terrain, access.
 - Economic environment: Finances, interest rates, general economy.
 - Government regulation: Laws, policies and regulations, real or impending.

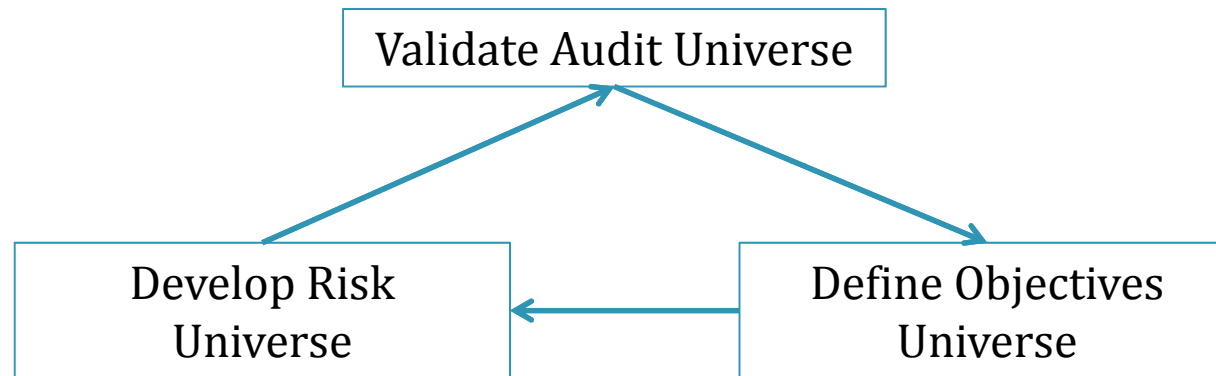
Identify Risks

- Develop the “Risk Universe” (Cont.)
 - Physical environment: Site, location, weather, terrain, access.
 - Competition: Direct competitors, substitutions, indirect competitors.
 - Constituents/Customers.
 - Suppliers (including unions).
 - Technology.
- Threat Scenarios/Brainstorming (see Handout): Special narrative speculation about how the system of internal control could possibly be defeated by fraud or natural disaster. Typically a risk framework is used to prompt risk thinking.

Identify Risks



Identify Risks





Identify Risks

- Reassess the Audit Universe
 - Additional information is often gathered in risk identification process
 - Validate the initial audit universe through review of:
 - Chart of Accounts
 - Organization Chart
 - Telephone Directory
 - Strategic Plan(s)
 - Information Systems Inventory
 - Audit Requests
 - External Benchmarking

Risk Assessment Process Overview

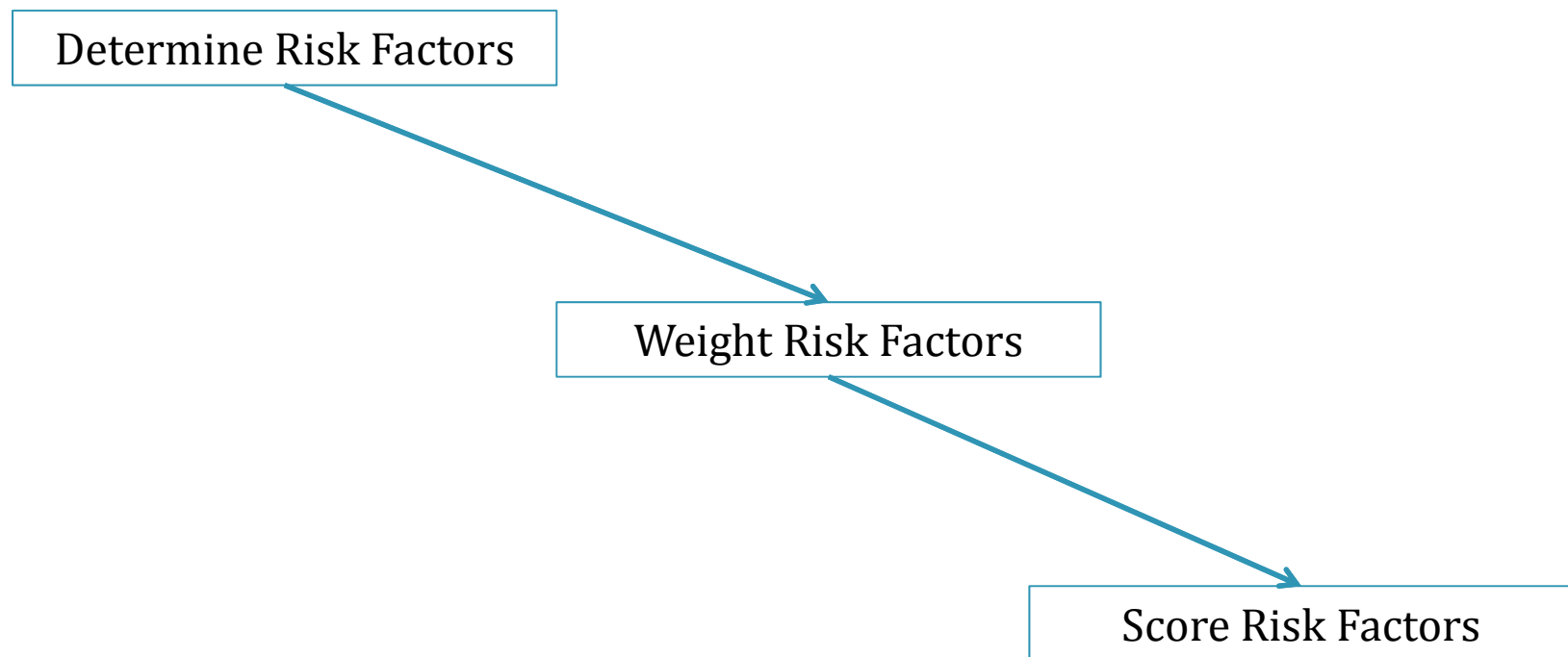




Measure Risks

- BEWARE!!! Risk measurement can be a “fool’s errand” due to Physics Envy and False Precision
- Measuring risk is not a precise science and is difficult because of its intangible nature.
- Focus on the overall objective; identification of high impact audits and audit program design.
- Often quick qualitative measurement (High, Medium, Low) is most effective.

Measure Risks





Measure Risks

- Determine Risk Factors
 - Risk is difficult to measure directly except by probability estimates, and even these are highly suspect without a lot of data on the consequences of each risk.
 - Risk factors are observable and/or measurable characteristics of risks that can combine the analysis of risks, consequences, and controls all at once into conceptual attributes to allow risk to be more easily measured.

Measure Risks

- Determine Risk Factors (Cont.)
 - There are three types of risk factors commonly in use:
 - Subjective risk factors
 - Due to the rapid changes in the complexity of both technology and organizations in recent decades, historical data has become less significant. Many auditable units change so much between audits that prior audit history is of little use.
 - Sound subjective judgment by an experienced practitioner is just as valid as any other method.
 - *Example:* Subjective Risk Factors: Integrity of management and Extent of rapid changes in processes.

Measure Risks

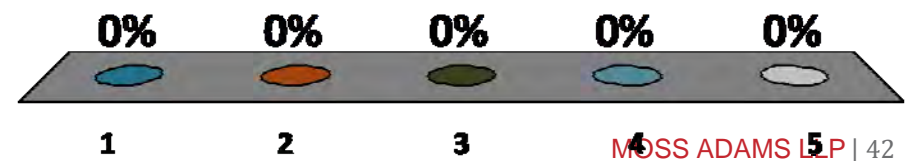
- Determine Risk Factors (Cont.)
 - Objective or historical risk factors
 - For stable operations, measuring the trends in historical risk factors can be useful. In all cases, current objective data are very helpful in measuring risk.
 - *Example:* Objective and Historical Risk Factors: Dollars at risk (Objective) and Employee turnover rates (Historical).
 - Calculated risk factors
 - A subset of objective risk factor data is the class of factors calculated from historical or objective data. These are often the weakest of all factors to use because they are derivative factors of risk further “upstream.” *Example:* Calculated Risk Factors: Distance from main office and Time since last audit.

Measure Risks

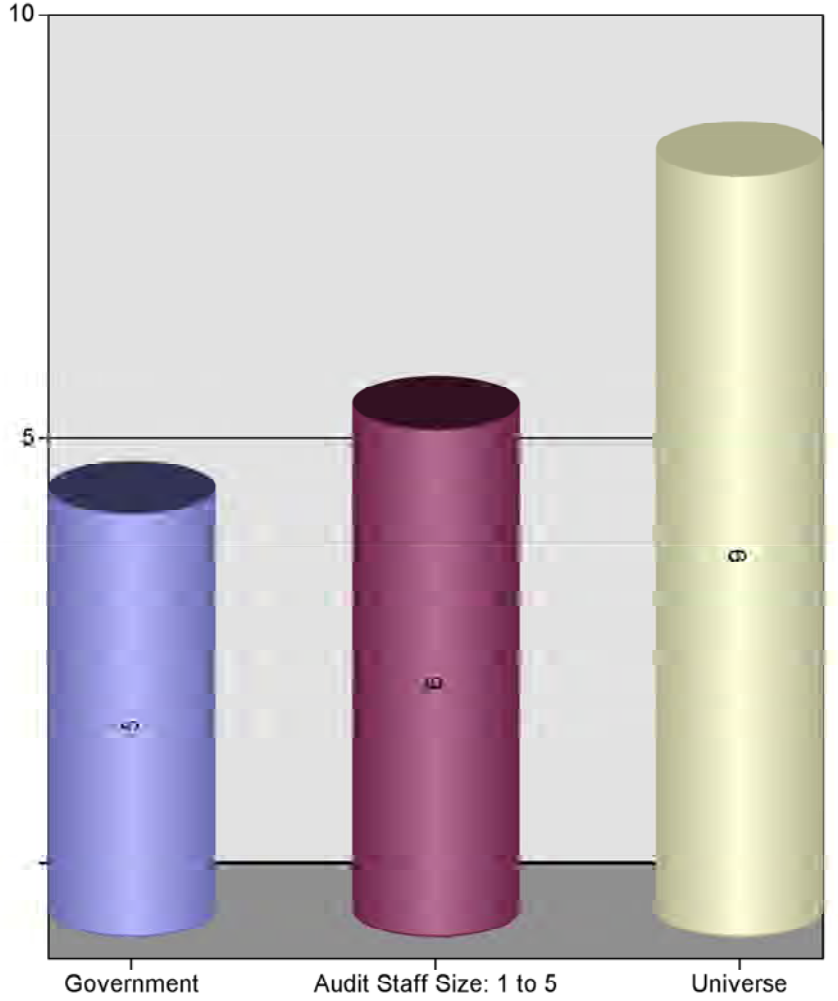
- Determine Risk Factors (Cont.)
 - These are often the weakest of all factors to use because they are derivative factors of risk further “upstream.”
 - *Example:* Calculated Risk Factors: Distance from main office and Time since last audit.
 - Caveat: Time since last audit is a very useful risk factor and we suggest that all risk assessment models include.
- Selecting Risk Factors
 - The IIA Practice Advisory 2010-2 outlines the need and appropriateness of using risk factors, in particular, a consideration of probability and impact of a risk.

How many risk factors do you use?

1. 11+
2. 8-10
3. 4-7
4. 1-3
5. 0



Number of Risk Factors Utilized



Source: IIA GAIN 2009 Benchmark Study

Factors Influencing Risk Assessment

Factor	Government	Audit Staff: 1 to 5	Universe
Degree of Financial Materiality	100%	84%	92%
Complexity of Activities	94%	79%	87%
Control Environment	94%	79%	89%
Reputational Sensitivity	92%	53%	69%
Inherent Risk	92%	72%	84%
Extent of Change	89%	84%	89%
Confidence in Mgmt	83%	61%	68%
Fraud Potential	81%	65%	81%
Time Since Last Audit	78%	67%	80%
Volume of Transactions	78%	65%	70%
Degree of Automation	72%	60%	72%

Source: IIA GAIN 2009 Benchmark Study

Factors Influencing Risk Assessment

Factor	Government	Audit Staff: 1 to 5	Universe
Employee Turnover	69%	56%	60%
Environmental Factors	64%	42%	48%
Other	22%	11%	17%
Competitive Pressures	17%	32%	36%

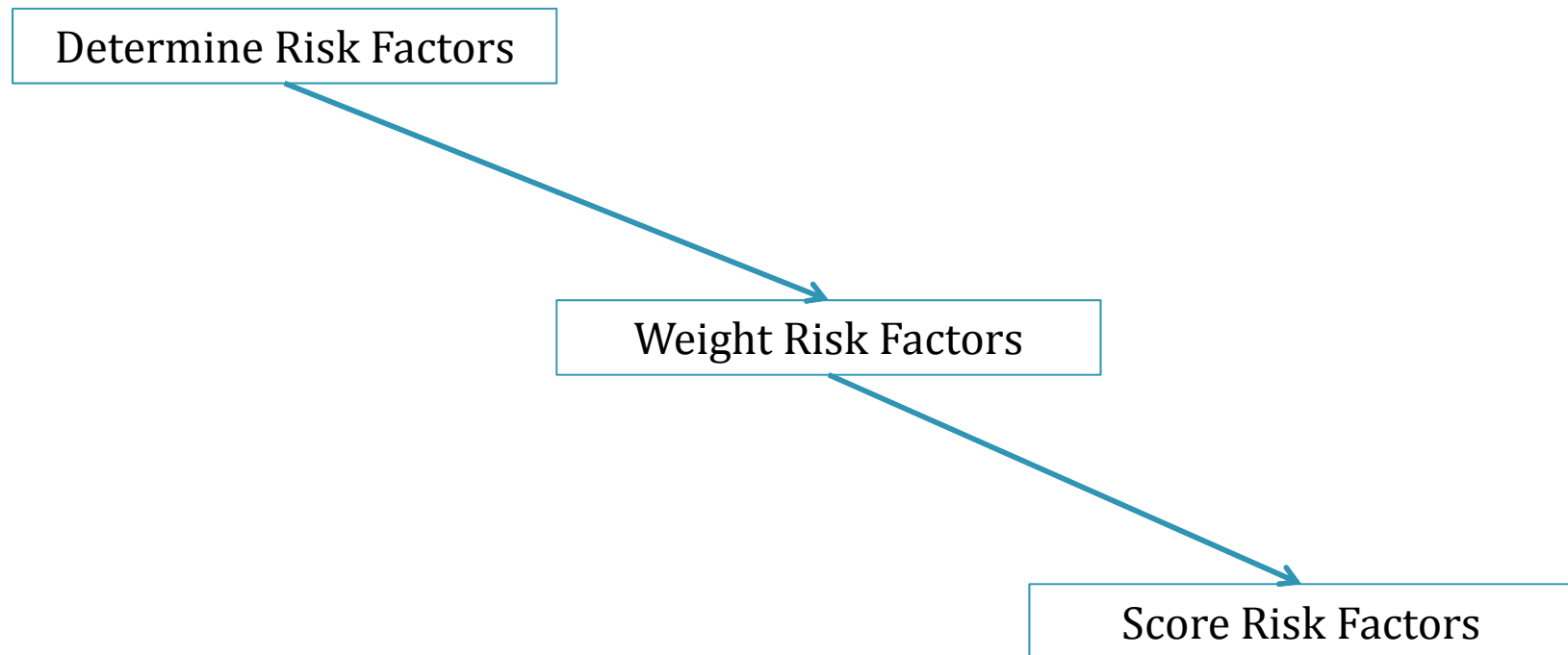
Source: IIA GAIN 2009 Benchmark Study



Measure Risks

- Determine Risk Factors (Cont.)
 - Choose a number of factors to represent important aspects of the auditable unit(s) risks.
 - These factors should be determinant. That is, the measurements on these factors should vary within each auditable unit from conditions of low risk to high risk.
 - Limit risk factors to no more than 10. Using 5, plus or minus 2, should be your goal. The more factors, the more likely you are duplicating the influence of a particular risk, and the less influence any particular factor has on determining ultimate risk.
 - See Handout for list of common risk factors.

Measure Risks

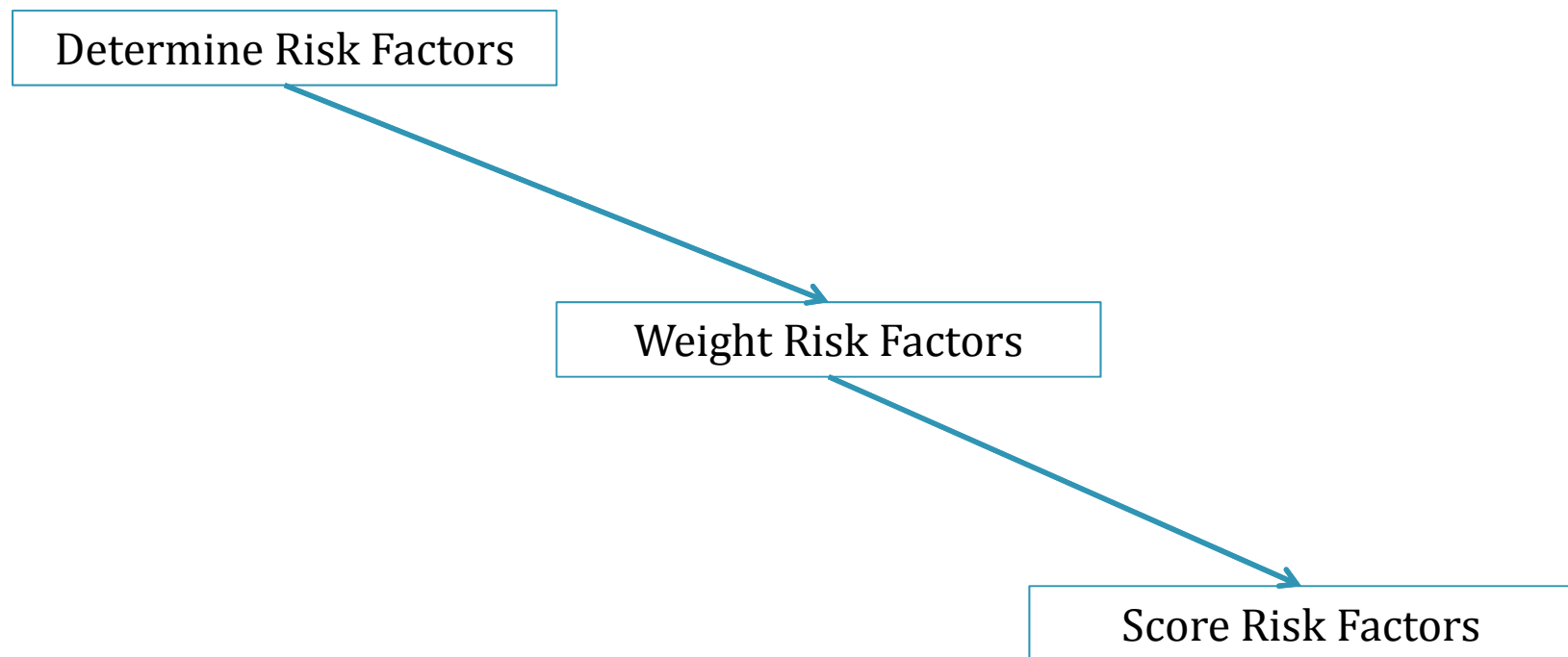




Measure Risks

- Weight Risk Factors
 - Reminder: This is a subjective process...budget efforts in this area accordingly.
 - Develop weights for each of the risk factors chosen based on the consequences that each factor has on the organization.
 - It is good practice to normalize the weights; that is, to make sure that the sum of all weights adds up to 1.00 or 100%.
 - Normally, a Direct Assignment method is used. Using judgment to determine the weight a particular factor should have in relation to other factors. Direct assignment can be done by the auditor or by a group using a consensus tool such as the Delphi Technique.

Measure Risks



Measure Risks

- Score Risk Factors
 - Choose a Scoring Scale - Choose a scale, such as “1-to-5,” to represent the strength of the factors in the auditable unit (low-to-high).
 - Document the criteria for rating for each risk factor
 - A five-point scale is recommended, although a three-point scale (low-medium-high, or weak average- strong) or even a 10-point scale can be used.
 - Evaluate each of the risks for the presence/absence or the relative strength/weakness of that risk factor and assign a score based on the scale selected.
 - Calculate the overall risk score by summing the product of each factor weight by its corresponding risk score.
 - The sum of the risk scores for each identified risk is called the “total risk”

Risk Assessment Process Overview





Prioritize Risks and Develop Audit Plan

- Prioritize Risks and Develop Audit Plan (Cont.)
 - There are three primary methods to select audits from the audit universe to include in the annual audit plan:
 - Cycle Approach.
 - Risk-Based Approach
 - Cycle-Based Risk Approach
 - The recommended Risk-Based Approach by mapping risks that relate to the same or similar Auditable Unit and could reasonable fit within the same audit program. For example, the audit on the next slide has a audit score of 153.

Prioritize Risks and Develop Audit Plan

- Prioritize Risks and Develop Audit Plan (Cont.)

Auditable Unit	Risk	Risk Score	Audit
Entity A Cash Disbursements	Inadequate segregation of duties between Vendor Invoice Entry and Cash Disbursements run	56	Entity A AP Cycle
Entity A Cash Disbursements	Accounts Payable check stock is not adequately secured.	35	Entity A AP Cycle
Entity A Accounts Payable	An approved PO or vendor invoice is not required before processing disbursements.	62	Entity A AP Cycle

Prioritize Risks and Develop Audit Plan

- Prioritize Risks and Develop Audit Plan (Cont.)
 - Once all risks have been mapped to relevant audits, the audits are then ranked from highest to lowest based on audit score.
 - The annual audit plan is chosen based on the percentage of “total risk” that is to be covered.
 - Typically a value between 50% to 75% is chosen.
 - The audits from the top of the list representing this point total are chosen. The balance of the auditable units is not included in the annual plan.
 - In the next example, the total risk is 628 and audits Nos. 1 and 2 (potentially 3) would be selected. The other audits may be scheduled for future years or left off completely.

Prioritize Risks and Develop Audit Plan

- Prioritize Risks and Develop Audit Plan (Cont.)

Audit	Audit Score
Audit 1	225
Audit 2 - Entity A Cash Disbursements	153
Audit 3	100
Audit 4	75
Audit 5	50
Audit 6	25



Key Points

- A risk-based audit planning approach is the key to adding value through internal audit.
- A risk-based audit planning process doesn't have to be arduous. Great is the enemy of good.
- Risk Identification is (by far) the most important (and difficult) step in the process.
- Over-reliance on an established Audit Universe can lead to a lack of risk-focus
- Risk Weighting and Scoring have rapidly diminishing returns. Beware "Physics Envy".

Questions?

Thank You!



MOSS ADAMS LLP

Certified Public Accountants | Business Consultants

Acumen. Agility. Answers.

The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.