Comprehensive Risk Assessment and Developing the Audit Plan

Laure Boyd, CIA, CGAP
Internal Audit Manager
Leon County Clerk of the Circuit Court and Comptroller
Our Time Today

- Background
- Risk Assessment and Audit Planning Process
  - Identify Risks
    - Develop 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
- Q&A
Priorities for internal audit:
1. Improving the risk assessment process
2. Enhancing the ability to monitor emerging risks
3. Becoming more relevant to achieving the organization's business objectives
4. Reducing overall IA function cost
5. Identifying opportunities for cost savings throughout the organization
Question?

- How many of you use a formal risk assessment process for internal auditing planning?
Definition of Risk

- Risk is the possibility that an event will occur and adversely affect the achievement of objectives – *COSO Definition*

- Risk - The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood - *IIA Standards Glossary Definition*
Definition of Risk continued

- Risk – is the combination of the probability of an event and its consequence.  *ISO/IEC 73*
Definition of Risk continued

- Risk is anything that could impact the achievement of objectives – not only negative impacts but also risk of missed opportunities.
What is the Goal of a Risk Assessment?

The risk assessment process should:

- Consider external and internal factors that could impact achievement of the objectives.
- Analyze the risks, and provide a basis for managing the risk.
- Allow auditors to focus efforts based upon risk in order to optimize efficiencies.
What is the Goal of a Risk Assessment?

continued, the risk assessment process should:

- Include consideration of technology supporting business processes and objectives.

- Be adapted to fit the pace of change in the organizational and market environment.
The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals.

*Interpretation:*

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive used his/her judgment of risk after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.
IPPF Performance Standard 2010.A1

“The internal audit activity’s plan of engagements much be based on a documented risk assessment, undertaken at least annually. The input of 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 the organization
- Generates buy-in from management
- Creates value
IIA Standards of Risk Management

2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

- 2120.A1- The internal audit activity must evaluate risk exposures relating to the organization’s governance, operations, and information systems.

- 2102.A2- The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
Risk Assessment and Developing the Audit Plan

- S. 20.055(5)(i), F.S., states in part:
  
  ...The Inspector General shall develop long-term and annual audit plans based on the findings of periodic risk assessments... The plan shall show the individual audits to be conducted during each year and related resources to be devoted to the respective audits...
What are some of the challenges in getting management buy in?
Signs For A Risk Assessment and Audit Planning Makeover

- Audit Plan is restricted to what “IA can audit today” vs. what “IA should audit tomorrow”.
- Audit plan included repetitive, low value audits.
- Administrative time makes up a significant portion of the audit plan.
- Internal audit and senior management’s views on risk prioritization are not aligned.
- Key processes, programs and initiatives are not linked to the organization’s strategic objectives.
- Audit plan excludes coverage of emerging risks or catastrophic Black Swan events that could impact the organization’s reputation.
Black Swan Event

Regulators allowed chemicals to slip through the cracks and poison the water supply.
Black Swan Event

Critics ask how can fewer than 3 inches of snow cripple the City of Atlanta?
Risk Assessment Process Overview

- Identify Risks
- Measure Risks
- Prioritize Risks
- Select and Develop Audits
Identify Risks

- Develop the Audit Universe
  - Audit Universe – The sum of all auditable units.
  - Auditable Unit – Parts of the organization that are exposed to sufficient risks where controls should be reviewed.
  - Develop the methodology for gathering information (I.e. who IA talks to, what information 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.
Identify Risks

- Develop the Audit Universe continued
  - Types of units: projects, IT systems, business functions, departments, business processes and sub processes, primary assets such as: physical, financial, human, intangible
  - Criteria for selecting Auditable Units
    - Contribute to the organizations goals
    - Sufficiently large to noticeably impact the organization
    - Sufficiently important to justify the cost of control
Identify Risks

- Define the Objectives Universe
  - What are the key objectives for each Auditable Unit?
  - Risks only exist in the context of the achievement of an objective. If you don’t know what the objective is you can’t identify the risk.
Identify Risks

Define the Objectives Universe Continued

- Categories of Objectives
  - Achievement of the organization's strategic objectives.
  - Reliability and integrity of financial and operational information.
  - Effectiveness and efficiency of operations.
  - Safeguarding of assets.
  - Compliance with laws, regulations, policies, procedures and contracts.
Identify Risks

- Develop the “Risk Universe”
  - If you don’t identify it you can’t measure, prioritize or manage it.
  - 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
      - Management questionnaires
      - Management interviews
Identify Risks

- Develop the “Risk Universe” continued
  - 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.
Identify Risks

- Develop the “Risk Universe” continued
  - Examples of Environmental Analysis:
    - Physical environment such as location, weather, access.
    - Economic environment such as finances, interest rates, general economy.
    - Governmental regulation such as laws, policies, regulations, real or impending.
  - Competition
  - Suppliers
  - Technology
Identify Risks

- Develop the “Risk Universe” continued
  - Threat Scenarios/Brainstorming
    - How can the system of internal control possibly be defeated by fraud or natural disaster?
Identify Risks

Brainstorm Schemes

- Payroll
- Credit Cards

Scenarios

- Payment to fictitious employee
- Payment to terminated employees
- Overpayment to existing employees
- Reimburse for personal expense
- Use card to circumvent competitive bid requirement
Identify Risks

- Reassess the Audit Universe
  - Additional information is often gathered in risk identification process.
  - Validate the initial audit universe through review of:
    - Organizational Charts
    - Strategic Plans and Initiatives
    - Annual Budget, Five-Year Financial Plan, and Capital Improvement Program
    - Performance Measures
    - Information Systems Inventory
    - Other
Measure Risks

- 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

- Determine Risk Factors
- Weight Risk Factors
- Score Risk Factors
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 all at once into conceptual attributes to allow risk to be more easily measured.
Measure Risks

- Selecting Risk Factors
  - The IIA Practice Advisory 2010-2 Using the Risk Management Process in Internal Audit Planning

- Outlines the need and appropriateness of using risk factors, in particular, a consideration of probability and impact of a risk.
What risk factors do you consider?

- Degree of Financial Impact/Materiality
- Complexity of Activities
- Management’s Confidence in its Systems of Internal Control
- Major Changes in Operations, Programs, Systems, or Controls
- Management’s Concerns and Public Perception
- Length of Time and Results of Previous Audits
Measure Risks

- **Weight Risk Factors**
  - This is a subjective process
  - Develop weights for each of the risk factors chosen based on the consequences that each factor has on the organization
  - Normalize the weights to make sure that the sum of weights adds up to 100%
  - Assign the weights. This can be done by the auditor or by a group using a consensus tool such as the Delphi Technique
Measure Risks

- Create buckets when assessing risks that face each business unit.
  - Audits
  - Internal Control Reviews
  - Validating Cash Narratives
  - External Audit
  - Observations and Suggestions Report
Measure Risks

- Score Risk Factors
  - Scoring Scale – Choose a scale to represent a low, medium or high probability
  - Document the criteria for rating each risk factor
  - A five-point scale is recommended although a three-point scale or even a 10-point scale can be used
  - Evaluate each of the risks for the presence/absence or the relative strength/weakness of the risk factor and assign a score based on the scale selected
Measure Risks

- Score Risk Factors continued
  - 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”.
Prioritize Risks and Develop the Audit Plan

- Prioritize Risks and Develop Audit plan
  - Once all risks have been mapped to relevant audits, the audits are then ranked from highest to lowest based on the audit score.
  - The annual audit plan is chosen based on the percentage of “total risk” that is to be covered.
  - The audits from the top of the list are chosen. The balance of the auditable units is not included in the annual plan or may be scheduled for future years or left off completely.
Create a Report of Other Observations and Suggestions

- Summarize by auditable unit notable items identified during the assessment process that management should be aware of for consideration and possible corrective action.
Communicate the Audit Plan

- Go over the results of the risk assessment with management to gain buy in and support.
- Go over the report of other observations and suggestions.
Makes Sense!

"If we always do what we’ve always done, we’ll always get what we’ve always gotten" Joseph T. Wells, Founder and Chairperson of the Association of Certified Fraud Examiners
Questions?

Laure N. Boyd, CIA, CGAP
Leon County Clerk of the Circuit Court and Comptroller
850-577-4221
LNBoyd@Leoncountyfl.gov