Finding the Risk in Risk Assessments
NYSICA
July 26, 2012

Presented by:

Ken Shulman

Internal Audit Director, New York State Insurance Fund

Risk Assessment

- There are different risk assessments prepared:
  - Annual risk assessment to develop the audit plan.
  - Enterprise Risk Management assessment.
  - Engagement planning risk assessment to identify specific areas to audit.
  - Others.

Risk Assessment

- Why are they done?
  - Comply with the Office of the State Comptroller's Standards for Internal Controls.
    - For agencies subject to OSC audits.
  - Address various professional standards.
    - Focus on the highest risks in an organization.
    - Meet management's needs.
    - Ensure objectivity in audits by using consistent measurements.

Risk Assessment

- The Risk Assessment is required by various auditing standards to meet the requirements for a risk-based audit plan.
- A risk assessment is not done to opine on the adequacy of controls. That is the purpose of an audit.
- A risk assessment is done to identify the highest risks and then develop a work plan.

Risk Assessment

- The Yellow Book requires auditors use professional judgment in planning and performing audits. (General Standards)
- It further requires that auditors adequately plan and document the planning of work necessary to address the audit objectives. (Field Work Standards relating to the engagement risk assessment.)

Risk Assessment

- Internal Audit Standards contain specific requirements for planning. Much more of a deep dive than GAGAS.
- Standard 2010 Planning - The Chief Audit Executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.

Risk Assessment

- Standard 2010.A1 requires that the IA annual audit plan should be based on a **documented** risk assessment, done at least **annually**.   The risk assessment should include **input from management and the Board**.
- This standard does not define sufficiency of documentation.

Risk Assessment

- Standard 2120.A1 requires that the internal audit activity evaluate risk exposures relating to organization's governance, operations, and information systems, regarding the:
  - Reliability and integrity of financial and operational information;
  - Effectiveness and efficiency of operations and programs;
  - Safeguarding assets; and
  - Compliance with laws, regulations, policies, procedures and contracts.

Risk Assessment

- Standard 2120.A2 requires the internal audit activity evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Risk Assessment

- The Internal Audit Standards Practice Advisory 2010-1 suggests linking the audit plan to risk and exposures. It offers that many Chief Audit Executives find it useful to develop an audit universe.
- An audit universe is a list of all possible audits that could be done by the Internal Audit Department.
- As new legislation and regulations are implemented, the audit universe is constantly evolving.

Risk Assessment

- Developing an Audit Universe
  - Need to break the agency/company into auditable components in order to focus the risk assessment. The risk assessment should not be at the 10,000 foot level.
  - Initially review agency information; mission statement, strategic plan, budget information, organization charts, annual reports, other audits conducted by external parties, compliance requirements, etc.
    - Previous risk assessments and audit plans.
    - Prior matrixes prepared by the Internal Control Office.
  - Review Intranet information updates discussing relevant topics.

Risk Assessment

- If an ERM was conducted/updated recently, obtain information from that.
  - Key Risk Indicators

Risk Assessments

- Internal auditors should not forget to include in their audit universe monitoring the process of the ERM as well as evaluating results and recommending improvements to the ERM.

- Internal Control Offices should review the identified risks in the ERM for completeness, as well as assist in identifying control activities to respond to risks.

Risk Assessment

- One suggestion is using questionnaires another is interviewing, and a combination of both of department heads for their input.
- There is no "one size fits all" approach. You have to assess what works best at your organization.
  - Involve Executive Management.
- Also, the approach depends on the maturity of the Internal Audit/Internal Control staff, stability of executive management, programmatic changes, etc.

Risk Assessment

- Questionnaires
  - If questionnaires are used, clear instructions should be provided to department heads. They need to understand what you are looking for - an example would help.
  - This may be time-consuming so Executive Management should have an understanding of the process.
    - Private companies, such as banks, insurance companies, brokerage firms are used to audits, but governments may not be by internal auditors, external auditors, regulators, investigators, etc.

Risk Assessment

- Questionnaires
    - They have to be kept to a high level in order to not overwhelm department heads.
- Ask the department managers to break out their auditable units. Use prior questionnaires as a starting point, unless this is the first time.
- Have them describe each auditable unit's purpose.
- Staffing changes.
- Revenue and expense information.
- Last audit and by whom (obtain a copy of the report).
- Significant changes in information reported between years.

Risk Assessment

- Ask managers to identify how their unit fits in with the entire organization.
- Fraud risk potential and potential impact.
- Supervisory staff changes and reasons (retirement, termination, etc.).
- Other information that you need to better understand the unit for preparing the risk assessment.
- Walk a fine line between obtaining enough information without overburdening unit management.
- Keep in mind that all risk is not necessarily bad. For example a higher investment risk is expected to yield a higher return.

RISK ASSESSMENT

- Review the questionnaires returned.
- A best practice could be to hold follow up discussions with each program manager, especially if they are new, or there were a number of changes in the area.
  - Develop a better understanding of how auditable units (functions) are determined.
  - Obtain information on functions to assist in classifying their risk.
  - Draw out other auditable units, that the unit head may not have thought about and obtain better clarity on perceived risks.

Risk Assessment

- After the meeting, auditors should assess whether they need to modify the questionnaires done by the department heads to recognize changes identified in the follow up meeting.
- Both versions of the questionnaire should be retained to document the changes and support the reasons for the changes.

Risk Assessment

- Risk rankings are generally based on two primary factors.
- Each risk needs to be evaluated based on these factors.
  - Likelihood
  - Impact

Risk Assessment

- Likelihood
  - Is the probability that an unfavorable event would occur.
    - Could this risk happen, would this happen?
    - For example if looking at inventory - could this desk be stolen?
    - Could this laptop computer be stolen?
    - If looking at staffing, key management staff nearing retirement age?
    - IT related problem/outage (keep in mind the upcoming data center consolidations)?
    - Budgetary cuts?
    - New program initiatives?

Risk Assessment

- Impact
  - The effect that an unfavorable event would have on the organization if an event occurred.
    - Consider management's risk appetite. If management has not developed its risk appetite, auditors should use their best estimate.
    - This can be measured by quantifiable measures (financial losses, for example, by poor controls), or it may not be quantifiable, such as reputational risk. Reputational risk could translate into a quantifiable risk. Also, understand inherent risk which is the risk affecting the agency if no action is taken.

Risk Assessment

- In government, the impact threshold seems to be a different definition than for privately held companies. It may not reconcile with risk appetite.
  - Agency reputations are damaged for insignificant amounts of lost value (cell phone usage, immaterial amounts of incorrect payments, etc.).
  - Don't lose track of material risks. Try to balance both types of risks.

Risk Assessment

- Translating the risk assessment into the audit plan.
- After completing the updated questionnaires, auditors should individually have an opportunity to review the information.
- A meeting can be held to help rank the risks by the audit team.
  - This technique helps to let each team member provide input and assure that the questionnaires support the team's risk conclusion.
  - Some risk ranking ideas include a risk numbering system (numerical value 1, 2, 3 etc.), or risk ranking system (high, medium, low).

Risk Assessment

- Not all risks should be ranked high. (Bell shaped curve?)
- Develop a heat map (four quadrants) to plot risks as a graphic.
- Some audit shops find it helpful to share a draft of the results of their risk assessment with Executive Management and the Audit Committee before finalizing.
  - Offers a chance for feedback (buy-in) before the audit plan is finalized.
  - Can modify the audit plan to include areas that Executive Management/Audit Committee want included.

Risk Assessment

- Once finalized, present the risk assessment to the Board and to Executive Management.
- Remember it is a living document and should be periodically monitored (does not have to be updated) for changes based upon circumstances (i.e., consolidation of various statewide functions in the Business Service Center).
- Especially important as you are identifying your next engagement.

Risk Assessment

- Other Considerations
  - Choosing medium or lower risks to examine
    - To confirm that the ranking was accurate.
  - Changes in regulations and their impact on the existing risk assessment.
  - External audit/investigations work and their results.
  - Executive Management changes. Management may make changes causing modified risks and want to shift focus.
  - Organizational changes (reorganizations).

Risk Assessment

- Another risk assessment conducted is the Enterprise Risk Management.
  - In 2004, COSO introduced its Enterprise Risk Management – Integrated Framework.
  - There are other ERM frameworks (ISO 3100-2009, Joint Australia/New Zealand 4360-2004, and the Turnbull Guidance).

RISK ASSESSMENT

- ERM is primarily an Executive Management and Board role.
  - ERM looks at risk enterprise-wide, breaking down the silos that exist within various departments/units.
  - ERM accepts that risks exist every day. Management must decide which risks to accept as a cost of doing business and which to mitigate based on risk appetite, and other factors.
  - Many of the factors are the same as those considered by conducting risk assessments as part of an audit planning process – likelihood and impact.

RISK ASSESSMENT

- A decision matrix can be used to identify risks affecting the organization.
  - The risk can be prioritized by likelihood and impact.
  - This will determine whether the risk falls within management's defined risk appetite.
  - The matrix also compiles information on each risk relating to which unit "owns" the risk, the planned response (accept, mitigate, etc.), the control activities, type of control (preventive vs. detective), whether the risk has been audited recently and by whom, and an estimate of the residual risk (what risk is left after the control activities and the risk response).

RISK ASSESSMENT

- Engagement risk assessment is conducted after an area is identified to audit.
- A survey of the area needs to be performed to focus the audit's scope to the most significant risk(s).
- Generally staff will follow a similar approach to the technique used to develop an audit plan.
  - Review external audits and investigations.
  - Review mission statements.
  - Review financial and programmatic information.
  - Obtain copies of organizational charts.

Risk Assessment

- Questions?