How to Kick-start your Audit Planning and Risk Assessment

Jaime Jue, Associate Director, UC Berkeley
David Meier, Manager–Campus Audits, UC San Diego
January 2013

Agenda

• Audit Project Process Overview
• Preliminary Survey and Risk Assessment
• Defining Risk
• Risk Assessment Framework Examples
• Challenges
• Q&A
Overview of the Audit Planning Process

From Project Flowchart – UC Audit Manual 6000.2

PREPARED FOR 2013 UC COMPLIANCE AND AUDIT SYMPOSIUM – FOR ADVANCED REVIEW PURPOSES ONLY

---

Notifying the Client

A member of the audit team should notify the parties responsible for an organization or area to be audited that an audit is scheduled using local audit office protocol. Notification should generally be sent via written memo or e-mail to the audit client with copies to senior officials as appropriate.

IPPF Performance Standard §2200
UC Internal Audit Manual 6000.03

PREPARED FOR 2013 UC COMPLIANCE AND AUDIT SYMPOSIUM – FOR ADVANCED REVIEW PURPOSES ONLY
Obtaining Client Input

Typically an entrance conference should be conducted with the client in order to discuss:
- Preliminary scope and objectives
- Management’s input as to what risks the audit should focus on

Communicating the Preliminary Scope and Objectives

The audit timing and preliminary objectives should generally be communicated to the client in writing in advance of the beginning of fieldwork. This information may be included in entrance meeting materials or other documents sent to the client.
What is the purpose of the Preliminary Assessment?

Internal auditors must develop and document a plan for each engagement, which must include:

- Objectives (§2210)
- Scope (§2220)
- Timing
- Allocation of Resources (§2230)

This plan is documented in an Engagement Work Program (§2240).

IPPF Performance Standards - Engagement Planning (§2200)
UC Internal Audit Manual 6000.01

Preliminary Audit Scope

Adequate audit planning requires that audit management define an appropriate preliminary audit scope that considers relevant systems, records, personnel, and the resources needed for the audit.

IPPF Performance Standards - Engagement Planning (§2200)
UC Internal Audit Manual 6000.02
Required Considerations for Understanding the Activity

Internal auditors must consider the following related to the activity being audited:

- Activity’s Objectives
- Significant Risk
- Risk Management and Control Processes
- Opportunities for Significant Improvements

Sources of Background Information

- Activity’s objectives and goals
- Policies, plans, procedures, laws, regulations and contracts having significant impact on operations
- Organizational information, such as number and names of employees, job descriptions, process flowcharts, details about recent changes, etc.
- Budget information, operating results and financial data
- Systems, records and physical properties including those controlled by a third party
- Prior audit work papers and reports
- Relevant authoritative and technical literature

Consideration of the Activity’s Objectives

- What are the objectives of the activity being reviewed?
- By what means does the activity control its performance?
Consideration of Significant Risks Associated with the Activity

- What are the significant risks to the activity's:
  - Objectives
  - Resources
  - Operations
- By what means are the potential impact of risk kept to an acceptable level?

Consideration of Management’s Risk Mitigation Efforts

Risk Management and Control Processes
- How adequate and effective are the activity’s risk management and control processes compared to a relevant control framework or model?

Consideration of Opportunities for Significant Improvement

What opportunities are there for making significant improvements to the activity’s risk management and control processes?
Refining the Audit Objectives

Objectives must be established for each audit including consideration of the following:

- Preliminary Risk Assessment
- Probability of Errors, Non-compliance or Fraud
- Criteria for Evaluating Controls

Preliminary Risk Assessment

- Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review
- Engagement objectives must reflect the results of this assessment
- Objectives should be phrased in terms of contributing to the organization properly managing the activity's risks through effective governance, risk management, and control practices

Preliminary Risk Assessment (cont'd)

Internal auditors consider:
- Management's assessment of risks relevant to the activities under review
- The reliability of management's assessment
- Management's process for monitoring, reporting, and resolving risk and control issues
- Management's reporting of events that exceeded the limits of the organization's risk appetite and management's response to those reports
- Risks in related activities relevant to the activity under review
Preliminary Risk Assessment (cont’d)

Internal auditors:

- Obtain and update background information about the activities to be reviewed or determine the impact on the engagement objectives and scope
- (If appropriate) conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis, and to invite comments and suggestions from engagement clients

Preliminary Risk Assessment (cont’d)

Internal auditors summarize the results from the reviews of management’s assessment of risk, the background information, and any survey work. This summary includes:

- Significant engagement issues and reasons for pursuing them in more depth
- Engagement objectives and procedures
- Methodologies to be used, such as technology-based audit and sampling techniques
- Potential critical control points, control deficiencies, and/or excess controls
- When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives

Using a Top-Down, Risk-based Approach to Identify Controls to Assess

- “Top-down” refers to basing the scope definition on the more significant risks to the organization
- A system of internal control typically includes both manual and automated controls
- The internal auditor needs to assess whether there is an appropriate combination of controls, including those related to IT, to mitigate business risks within organizational tolerances
- The internal auditor needs to consider including procedures to assess and confirm that risk tolerances are current and appropriate
Using a Top-Down, Risk-based Approach to Identify Controls (cont’d)

- The scope needs to include all the controls required to provide reasonable assurance that the risks are effectively managed. These controls are referred to as key controls.
- Only key controls need to be assessed.

Key controls can be in the form of:
- Entity-level controls
- Manual controls
- Fully automated controls
- Partly automated controls

If the audit scope includes some, but not all, key controls required to manage the targeted risks, a scope limitation should be considered and clearly communicated in the internal notification and final report.

Considering Probability of Errors or Fraud

Internal auditors must consider the probability of:
- significant errors,
- fraud,
- noncompliance, and
- other exposures
when developing the engagement objectives.
Establish Control Evaluation Criteria

- Adequate criteria are needed to evaluate controls
- Internal auditors must ascertain the extent to which management has established criteria to determine whether objectives and goals have been accomplished
- If adequate, internal auditors must use such criteria in their evaluation criteria
- If inadequate, internal audit must work with management to develop appropriate evaluation criteria

IPPF Practice Advisory PA2200-2

Refining the Engagement Scope

The established scope must be sufficient to satisfy the objectives of the engagement:

Consideration of Relevant Systems and Personnel

Opportunities for Consulting

IPPF Performance Standards - Engagement Scope (§2220)

Consideration of Relevant Systems and Personnel

The scope of the engagement must include consideration of:
- Relevant systems
- Records
- Personnel
- Physical properties (including those under the control of third parties)
Consulting/Advisory Opportunities

If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the:

- objectives,
- scope,
- respective responsibilities, and
- other expectations
should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

Engagement Resource Allocation

- Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.
- An important element of any audit budget generally includes time for the auditor assigned to learn about new systems and processes.
- Audit management may also consider the use of external resources, where knowledge, expertise and staffing is lacking.

IPPF Standard §2230 / UC Audit Manual 6100.04

Developing the Audit Program
Engagement/Audit Program

Internal auditors must develop and document work programs that achieve the engagement objectives. A completed engagement program must:

- State the objectives of the audit
- Identifies technical requirements, objectives, risks, processes, and transactions that are to be examined
- States the nature and extent of testing to be required
- Documents the procedures for identifying, collecting, analyzing, interpreting, and documenting information during the engagement

Approving the Audit Program and Beginning Fieldwork

Approval of and Modifying the Audit Program

- Audit management generally approves the audit program at the end of the preliminary survey.
- If there are adjustments to the program, these adjustments should be approved by audit management prior to beginning the related fieldwork.
- Changes to the audit budget should be formally agreed to by audit management as early in the audit timeline as possible.

IPPF Practice Advisory - Engagement Work Program (§2240)
UC Audit Manual 6100.04
Defining Risk

- Anything that may get in the way, and prevent management from achieving its objectives
- Related to opportunity — mirror views
- Functional owner versus independent reviewers’ perspectives (internal and external)
- Pervasive internal control weakness or lack of management control or accountability
- Publicly or politically sensitive area
- Regulatory requirements — potential fines & penalties
- Potential for high dollar impact or loss
- Organizational gaps (i.e., org. restructures)

Types of Risk

- Financial
  - Stewardship for public funds
  - Efficiency in use of funds
  - Accuracy of financial reporting
- Operational
  - Effectiveness in achieving objectives
  - Compliance — regulatory risk
  - Fines, penalties, sanctions
  - Information technology and data
  - Security for IT resources — multiple levels
  - Data privacy
Defining Risk – Local Context

- Centralized versus decentralized
- Amount of federal funding (EMF = $1B)
- Other relevant regulatory risks
- Management style – consensus driven
- Org. culture and communications
- Change drivers
- Academic vs. administrative stakeholders
- IT infrastructure

Risk Assessment Frameworks - Examples

- Internal Control Questionnaires (by topic)
- Separation of Duties Matrices
- Analytical review procedures
  - Department permanent budget information
  - Contract & grant activity
  - Department financial snapshots - sources & uses of funds (examples)
  - Data extraction and analysis
  - Control gap analysis (examples)

Risk Assessment Frameworks – Financial Snapshot 1

<table>
<thead>
<tr>
<th>Account Category</th>
<th>Susp</th>
<th>Assets</th>
<th>Self</th>
<th>DOM</th>
<th>New</th>
<th>Old</th>
<th>MD</th>
<th>Equipment</th>
<th>New</th>
<th>Transfer</th>
<th>Isolated</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Funds</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Separated, Principal Appropriated Funds</td>
<td>10,882</td>
<td>1,894</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Separated, Operating Funds</td>
<td>1,203</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Student Aid</td>
<td>3,171,788</td>
<td>76,403</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Self-Dependent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Self-Supporting</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Self-Dependent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Self-Dependent</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>12,245,996</td>
<td>12,753,108</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

 presidente: 3

$5,043,208

Salaries and Benefits - % of total $89.2%
Risk Assessment Frameworks – Financial Snapshot 2

<table>
<thead>
<tr>
<th>Category</th>
<th>Source 1</th>
<th>Source 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salaries</td>
<td>323,274</td>
<td>288,400</td>
</tr>
<tr>
<td>Donations</td>
<td>913,223</td>
<td>66,178</td>
</tr>
<tr>
<td>Private Student</td>
<td>251,860</td>
<td>95,349</td>
</tr>
<tr>
<td>Principal Opportunity</td>
<td>31,087</td>
<td>0</td>
</tr>
<tr>
<td>State General</td>
<td>302,509</td>
<td>3,283</td>
</tr>
<tr>
<td>Benefits</td>
<td>818,444</td>
<td>0</td>
</tr>
<tr>
<td>Grants</td>
<td>66,178</td>
<td>0</td>
</tr>
<tr>
<td>Gifts</td>
<td>25,649</td>
<td>0</td>
</tr>
<tr>
<td>Grants</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>33,095,390</td>
<td>1,315,739</td>
</tr>
</tbody>
</table>

Risk Assessment Frameworks – Gap Analysis 1

<table>
<thead>
<tr>
<th>Description</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial snapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validate financial snapshot with expected budget and actual expenditures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze financial snapshot for accuracy and completeness.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Assessment Frameworks – Gap Analysis 2

<table>
<thead>
<tr>
<th>Section</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial snapshot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validate financial snapshot with expected budget and actual expenditures.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze financial snapshot for accuracy and completeness.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1/18/2013
Risk Assessment Challenges

Some potential challenges:
- Audit topics crossing organizational boundaries
- Departmental vs. central process/system owners
- Organizational gaps - identifying control owners
- Identifying decision makers
- Differing risk tolerances/appetites
- Quantifying or benchmarking risk
- The reluctant client
- Position of IA in the organization & resources

How to Kick-start your Audit Planning and Risk Assessment

Q&A
Thank You!
How to Kick-start your Audit Planning and Risk Assessment

Speaker Contact Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>E-mail</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jaime Jue</td>
<td>Associate Director</td>
<td><a href="mailto:jguj@berkeley.edu">jguj@berkeley.edu</a></td>
<td>510-642-2064</td>
</tr>
<tr>
<td>David Meier</td>
<td>Manager – Campus Audits</td>
<td><a href="mailto:dmeier@ucsd.edu">dmeier@ucsd.edu</a></td>
<td>858-534-1334</td>
</tr>
</tbody>
</table>

This presentation was prepared solely for delivery at the University of California’s Ethics, Compliance, and Audit Services 2013 Compliance and Audit Symposium. It is intended to supplement a more comprehensive live, in-person presentation. The information contained herein is of a general nature and is not intended to address the circumstances of any particular campus, unit, or individual. Although every endeavor is made to provide accurate and timely information, there can be no guarantee that such information is complete or up-to-date. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.