2013 Compliance and Audit Symposium

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

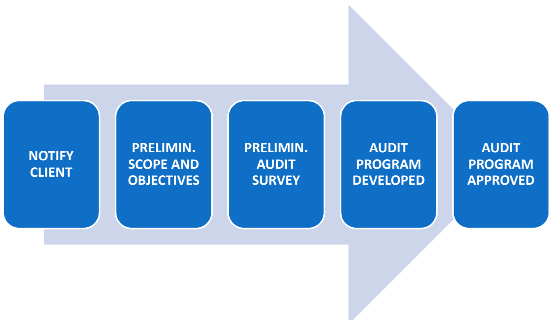
 2

How to Kick-start your Audit Planning and Risk Assessment

Audit Project Process Overview

 3

Overview of the Audit Planning Process

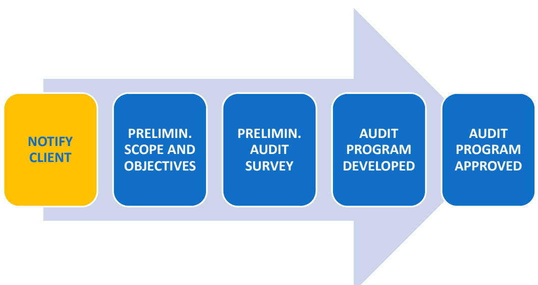


From Project Flowchart – UC Audit Manual 6000.2

4

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

Notifying the Client



5

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

6

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

Obtaining Client Input

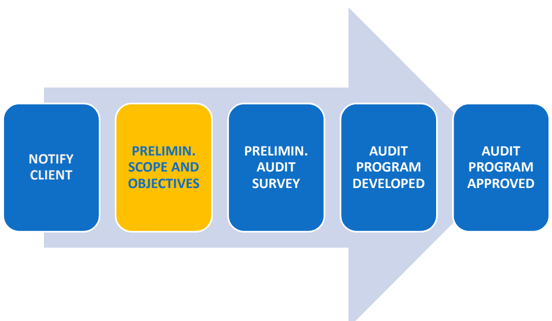
Typically an entrance conference should be conducted with the client in order to discuss:

- Preliminary scope and objectives
- Management's input as to what risks the audit should focus on

UC Internal Audit Manual 6100.03

 7

Preliminary Scope and Objectives



 8

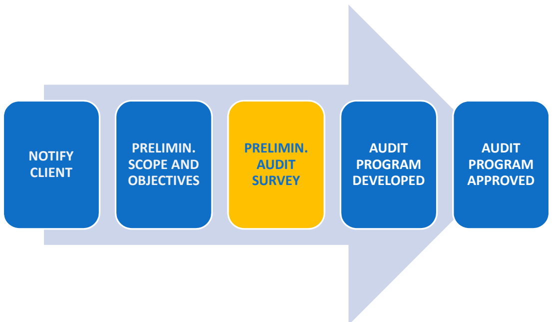
Communicating the Preliminary Scope and Objectives

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.

IPPF Performance Standards - Engagement Planning §2200
UC Internal Audit Manual 6000.03

 9

Preliminary Audit Survey



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

IPPF Standard §2200
UC Internal Audit Manual 6000.2

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

UC Internal Audit Manual 6100.4

Consideration of the Activity's Objectives

- What are the objectives of the activity being reviewed?
- By what means does the activity control its performance?

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

IPPF Performance Standards - Planning Considerations (§2201)
UC Audit Manual 6000.02

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?

IPPF Performance Standards - Planning Considerations (§2201)
UC Audit Manual 6000.02

16

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

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?

IPPF Performance Standards - Planning Considerations (§2201)
UC Audit Manual 6000.02

17

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

Consideration of Opportunities for Significant Improvement

What opportunities are there for making significant improvements to the activity's risk management and control processes?

IPPF Performance Standards - Planning Considerations (§2201)
UC Audit Manual 6000.02

18

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

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

IPPF Performance Standards - Engagement Objectives (§2210)

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 | Probability of Errors, Non-compliance or Fraud | Criteria for Evaluating Controls

IPPF Performance Standards - Engagement Objectives (§2210)

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 | Probability of Errors, Non-compliance or Fraud | Criteria for Evaluating Controls

IPPF Practice Advisory (PA §2210) - Risk Assessment in Engagement Planning

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

IPPF Practice Advisory (PA §2210) - Risk Assessment in Engagement Planning

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

IPPF Practice Advisory (PA §2210) - Risk Assessment in Engagement Planning

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

IPPF Practice Advisory PA2200-2

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

IPPF Practice Advisory PA2200-2

Using a Top-Down, Risk-based Approach to Identify Controls (cont'd)

- 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

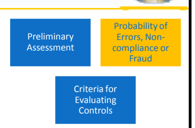
IPPF Practice Advisory PA2200-2

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



IPPF Practice Advisory PA2200-2

Establish Control Evaluation Criteria

Preliminary Assessment | Errors, Non-compliance or Fraud | Criteria for Evaluating Controls

- 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

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

28

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)

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

29

Consideration of Relevant Systems and Personnel

Consideration of Relevant Systems and Personnel | Opportunities for Consulting

The scope of the engagement must include consideration of:

- Relevant systems
- Records
- Personnel
- Physical properties (including those under the control of third parties)

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

30

Consulting/Advisory Opportunities

Consideration of Relevant Systems and Personnel

Opportunities for Consulting

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

- objectives,
- scope,
- respective responsibilities, and
- other expectations

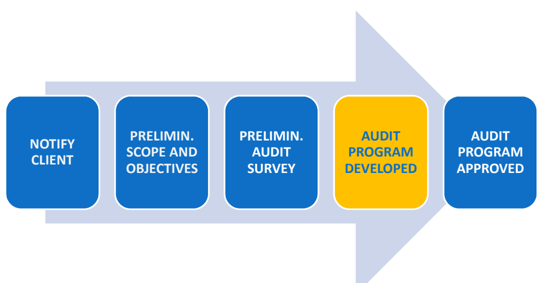
should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

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

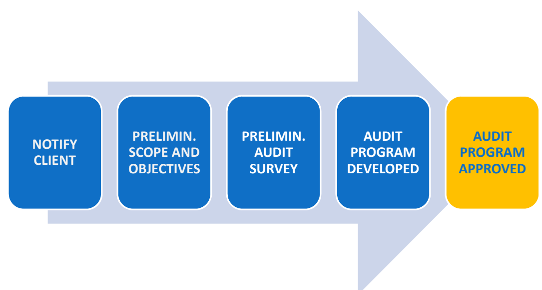
Internal auditors must develop and document work programs that achieve the engagement objectives.

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

IPPF Practice Advisory PA2200-1
UC Internal Audit Manual 6100.4

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

How to Kick-start your Audit Planning and Risk Assessment

Defining Risk

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

Fund Assignment	Expenses	Academic	Staff	Gen. Asst.	Benefits	S&E	Equipment	Travel	Transfers	Unallocated	Overhead
Agency Funds	64	0	0	0	0	64	0	0	0	0	0
Endowment - Principal Appropriated Funds	19,418	1,999	0	0	35	12,678	0	4,706	0	0	0
Opportunity Funds	148,433	5,083	0	500	118	136,959	0	5,772	0	0	0
Principal Appropriated Funds	0	0	0	0	0	0	0	0	0	0	0
Student Fees	113,772	70,467	0	600	5,071	37,201	0	434	0	0	0
Private Gifts and Grants, Unrestricted	0	0	0	0	0	0	0	0	0	0	0
Self-Supporting Activities	-15	0	0	0	0	-15	0	0	0	0	0
General Funds	5,173,998	3,355,113	658,663	78,149	803,078	218,201	10,330	50,464	0	0	0
State Appropriation	61,687	36,208	0	0	2,521	21,508	0	1,451	0	0	0
Federal Funds	**17,304**	**0**	**0**	**5,206**	**0**	**12,099**	**0**	**0**	**0**	**0**	**0**
Private Gifts	97,051	16,811	0	0	3,586	66,153	0	10,291	210	0	0
Private Contracts	22,576	0	0	0	0	20,524	0	0	0	0	2,052
Private Grants	0	0	0	0	0	0	0	0	0	0	0
Totals	5,654,288	**3,485,681**	**658,663**	**84,455**	**814,408**	525,370	10,330	73,118	210	0	2,052
Salaries and Benefits - $	5,043,208										
Salaries and Benefits - % of total $	89.2%										

Risk Assessment Frameworks – Financial Snapshot 2

Fund Assignment	Expenses	Academic	Staff	Gen. Asst.	Benefits	S&E	Equipment	Travel	Transfers	Unallocated	Overhead
Agency Funds	0	0	0	0	0	0	0	0	0	0	0
Opportunity Funds	275,255	80,363	0	4,078	13,559	237,554	-63,878	3,578	0	0	0
Principal Appropriated Funds	581,074	63,893	851	0	22,641	188,409	0	12,451	292,829	0	0
Student Fees	537,413	244,627	0	84,836	23,366	184,584	0	0	0	0	0
Private Gifts and Grants, Unrestricted	0	0	0	0	0	0	0	0	0	0	0
Self-Supporting Activities	1,934,842	7,302	691,606	45,406	324,738	888,238	201,933	33,632	-258,013	0	0
Contract and Grant Administration	-25,835	-6,602	-268	9,146	-5,418	-23,111	0	400	18	0	0
Reserves	0	0	0	0	0	0	0	0	0	0	0
General Funds	22,397,485	11,578,360	3,464,442	536,000	3,419,525	2,287,038	657,242	349,326	105,552	0	0
State Appropriation	336,179	163,842	-10,842	925	50,234	71,125	40,597	20,298	0	0	0
Federal Funds	**33,095,390**	**7,216,532**	**1,774,824**	**439,444**	**2,444,693**	**9,771,133**	**1,315,739**	**328,836**	**-206,501**	**0**	**10,010,691**
Donations and Gifts	200,658	80,181	13,070	8,432	22,347	73,645	-1,009	3,992	0	0	0
Private Federal Flow Thru	**608,793**	**166,712**	**55,117**	**7,013**	**68,350**	**85,203**	**-1,411**	**12,538**	**0**	**0**	**215,272**
Private Gifts	1,602,657	427,379	155,271	52,752	194,044	395,943	-7,590	45,451	11,883	0	327,522
Private Contracts	2,935,822	1,266,448	158,194	24,301	402,734	450,744	30,818	37,113	0	0	565,471
Private Grants	2,575,147	913,223	251,860	31,087	302,509	818,444	66,178	25,649	3,283	0	162,913
Plant Funds	-32,125	0	0	0	0	8,272	72,823	0	-113,220	0	0
Totals	67,022,755	22,202,259	6,554,125	1,243,419	7,283,324	15,437,221	2,311,441	873,264	-164,167	0	11,281,868
Salaries and Benefits - $	37,283,127										
Salaries and Benefits - % of total $	55.6%										

Risk Assessment Frameworks – Gap Analysis 1

Assertion	Risk	Controls	Residual Risk	Residual Risk Level
Timeliness	Report is not filed in a timely manner (10 days following the end of the reporting period).	Pis are required to submit their information at least 5 days in advance. Reporting Specialists are responsible for updating FederalReporting.gov. Timeliness is closely monitored by the ARRA reporting team.	PI's may not return the questionnaire.	**Medium.** If the information is late or inaccurate, University can correct for 10 days following the intial deadline. Hybrid staffing model further mitigates risk.
Completeness	Report did not include all ARRA awards.	ARRA Awards are uniquely coded in IFIS. Number of awards included in UCSD's report is reconciled to the ARRA awards listings on the NIH and NSF websites.	Non NSF or NIH award not properly identified as ARRA by OCGA staff would lead to the award not being included in the University's quarterly report.	**Medium** - ARRA awards are easily identified by staff. Lead Specialists check agency websites to determine if all awards were reported on in the FederalReporting.gov website.
Completeness	Sub-award/Vendor data was not included in the reports.	System used by Procurement automatically flags sub-award or PO's that are requested using ARRA funds. Information is sent to ARRA reporting team when a subaward or PO over $25K is processed. PI's are responsible for reporting Subaward and Vendor over $25K data, and reporting specialists verify via query that the data is complete.	Procurements may not properly flag sub awards as ARRA, resulting in missing sub-award language, as well as not informing the reporting team of the award. Purchase of over $25K may be broken down into more than one PO, resulting in vendor not properly being identified as as recipient of over $25k of ARRA funding.	**Medium** - Customized queries mitigate potential omission.
Accuracy	**Jobs** created/maintained is inaccurate or not calculated correctly. (Campus)	Although PI's are responsible for reporting this information to Reporting Specialists, the Specialists review the number by recalculating.	Human error on the part of Reporting Specialists and/or PI's.	**High** - Due to sensitivity of the data being reporting.
Accuracy	**Expenses** are not reported accurately.	Specialists use the ARRA Reporting query to obtain IFIS expenditure information.	Data entry error on the part of the reporting specialists	**Low** - Standardized financial queries have been used extensively by reporters.

Risk Assessment Frameworks – Gap Analysis 2

Business Objective: UCSD is required to provide and maintain a safe environment for its students, academic appointees, staff, visitors, and surrounding communities (PPM 516-19).

Business Risks (& Corresponding Functional Activity)	*Procedures in Place to Mitigate Risks*	*Residual Risk Assessment*	*Audit Procedures*
The organizational structure for campus oversight of safety provided by **EH&S and Safety Committees** may not be optimized to provide effective oversight of the laboratory safety program based on actual laboratory inspection findings.	Committees have been established to advise the Chancellor through the VC-RM&P on the safe use of chemicals; hazardous biological material and organisms and/or recombinant DNA; laser safety; radiation safety; and health, safety, and environmental protection at UCSD.	High – Based on preliminary responses from EH&S management, reporting is not provided to the committees or management outside of EH&S or the academic Vice Chancellor or Deans for the audited laboratories regarding laboratory inspection results. In addition, this was an area of weakness identified in the UCLA incident.	AMAS will: • Administer an electronic survey of safety committee members regarding laboratory safety oversight; • Conduct survey follow-up interviews of committee members based on the survey results; • Evaluate safety monitoring and reporting.
The personnel assigned as **Department Safety Officer (DSO), and Area Safety Coordinators** (ASC), may not fulfill their responsibilities.	Laboratory safety inspections are periodically performed (based on risk) to ensure the safety of the laboratory and compliance with policies. In addition, follow up is performed on laboratory inspection deficiencies to ensure that the deficiency is resolved.	High – DSO and ASC responsibilities are often performed in addition to the individuals' other responsibilities without additional compensation. There is a risk that safety activities are not highly prioritized.	AMAS will: • Administer an electronic survey of DSOs and ASCs regarding safety practices; • Analyze a sample of laboratory audit scores and/or violations; • Participate as an observer in a number of EH&S laboratory inspections; and • Evaluate the effectiveness of the DSO/ASC role and model.

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

Risk Assessment Challenges

- What types of challenges do you face in your risk assessments?
- How do you overcome those challenges?

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

Name	Title	E-mail	Telephone
Jaime Jue	Associate Director	jgjue@berkeley.edu	510-642-2064
David Meier	Manager – Campus Audits	dmeier@ucsd.edu	858-534-1334

49