

The Regents of the University of California

COMMITTEE ON COMPLIANCE AND AUDIT

March 17, 2015

The Committee on Compliance and Audit met on the above date at UCSF–Mission Bay Conference Center, San Francisco.

Members Present: Regents Engelhorn, Makarechian, Ruiz, Sherman, and Zettel; Advisory member Gilly; Staff Advisors Acker and Coyne

In attendance: Regent Leong Clancy, Regent-designate Davis, Faculty Representative Hare, Secretary and Chief of Staff Shaw, General Counsel Robinson, Chief Compliance and Audit Officer Vacca, Executive Vice President and Chief Financial Officer Brostrom, Vice President Sakaki, Chancellor Hawgood, and Recording Secretary Johns

The meeting convened at 11:20 a.m. with Committee Chair Zettel presiding.

1. APPROVAL OF MINUTES OF PREVIOUS MEETING

Upon motion duly made and seconded, the minutes of the meeting of November 18, 2014 were approved.

Committee Chair Zettel announced that earlier that morning in closed session, the Committee had appointed Eric Juline as its Expert Financial Advisor. Mr. Juline is an alumnus of UCLA and served as an alumni Regent in 2005-06. He is a retired partner of PricewaterhouseCoopers. The Committee was most grateful that he is willing to serve the public and the Regents and to share his expertise. Regent Engelhorn explained that Mr. Juline would serve without compensation. Committee Chair Zettel confirmed that he would be volunteering his services.

2. APPROVAL OF EXTERNAL AUDIT PLAN FOR THE YEAR ENDING JUNE 30, 2015

The President of the University recommended that the KPMG external audit plan and fees for the University for the year ending June 30, 2015, as shown on pages 4 and 13 of Attachment One, respectively, be approved.

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Associate Vice President and Systemwide Controller Peggy Arrivas explained that the scope of the external audit plan being recommended in the current year was the same as it had been the previous year. There were no required changes.

Mr. Mark Thomas of KPMG noted that the proposed fees were consistent with the contract the University and KPMG entered into a year previously.

Committee Chair Zettel asked how KPMG would determine which campuses to visit and what areas to review. Mr. Thomas responded that in the financial statement audit, KPMG would naturally focus on areas with the largest dollar amounts and the greatest cash flow, such as investment portfolios, student tuition and fees, and payroll costs. In addition, KPMG is required to introduce some surprise or changes to its audit. No entity or unit is exempt from audit procedures.

Regent Makarechian asked about audits of construction contracts, which were not mentioned in the background materials provided, as well as other areas of concern such as student health, the UCPath project, and sexual harassment prevention. Mr. Thomas responded that construction contracts are part of what could be selected for auditing in the financial statements. KPMG's work included construction, specifically construction compliance and review of major projects. In student health, KPMG carries out procedures related to the Student Health Insurance Program and provides a separate report, which was included in a list of additional reports in the background materials. Construction audits would be considered additional scope, related to construction compliance work KPMG is carrying out. While this was not specifically mentioned among KPMG deliverables in the background materials, it is a part of the overall projects KPMG performs for the UC system. Ms. Arrivas added that UCSF asked KPMG to perform a special project, additional audit-related procedures beyond what was required for the financial statements.

Regent Makarechian stressed that UC's annual construction budgets represent an enormous dollar amount and asked why this category was not specifically mentioned in the audit deliverables. Mr. Thomas responded that KPMG performs a substantial amount of work related to construction. Construction was not included in the list of deliverables because the list primarily concerned items involving judgment, such as assessment of market values of investments and pension liabilities. Mr. Thomas added that construction could be included in the list of deliverables and that he would comment on this topic when the audit was completed.

Regent Makarechian asked about KPMG's definition of materiality. Mr. Thomas responded that there was not a dollar definition of materiality per se. Materiality concerns any error identified that could have a significant impact on a reader of the financial statements. There is a substantial amount of judgment in making this determination. KPMG performs a number of calculations regarding materiality to determine when something becomes material. The actual materiality threshold varies by area. KPMG has calculated a materiality threshold based on each of the reports issued, for the medical centers, foundations, for the UC Retirement Plan, and for the system as a whole. KPMG continually strives to understand what level of error would have a significant impact on a reader of the financial statements.

Regent Makarechian asked that this definition of materiality be included in KPMG's audit proposal.

Committee Chair Zettel commented that KPMG would be examining information technology security and risk. KPMG had identified this as an area of concern several times during its work with UC, for example, regarding the issue of user access to UC financial systems. She hoped that KPMG would continue to pursue information technology security practices at UC, noting that the University does not always have the resources to purchase the most up-to-date technology.

Regent Ruiz recalled that UC was working on a number of efficiency projects such as UCPath. He asked what KPMG's role would be in this process. Mr. Thomas responded that KPMG was paying close attention to the progress of UCPath. Before the first UCPath implementation occurs, KPMG would like to ensure that appropriate controls are in place. KPMG was considering the possible scope of work for auditing the UCPath system immediately before or after its release or trial run. KPMG was fully engaged in this matter, but still determining when it should begin with test work and procedures.

Regent Ruiz asked about how KPMG would comment on the success or failure of UCPath or UC construction projects. Mr. Thomas responded that his familiarity with the UCPath project was not extensive enough to provide a comment. The campus construction projects at UCSF were going well, in his view. Regent Ruiz underscored the importance of receiving feedback from KPMG on significant UC projects.

Regent Makarechian asked that KPMG report in detail on the status of the UCPath project, and how and why the project has gone over budget and over time.

Regent Sherman asked about KPMG's work on investment valuation. He asked if there was sufficient transparency regarding UC investments, including private equity and venture capital. Mr. Thomas emphasized the enormity and complexity of the UC investment pool, and responded that there was adequate transparency. Given its status as a large investor, the University has power to request and demand information about funds.

Regent Sherman asked if there would be a footnote regarding Level One, Two, and Three valuations. Ms. Arrivas responded that this was a question about the disclosure requirement regarding public companies. The Governmental Accounting Standards Board (GASB) had recently, within the past few weeks, issued a new statement that would require Level One, Two, and Three disclosures for the market values of investments. This requirement would not be effective until 2016. Level One securities are those that trade on an open market and for which a market value is readily available in sources such as the *Wall Street Journal*. There are publicly available data for Level Two securities, but one cannot retrieve information about an individual security. One can look up data on interest rates for these securities and extrapolate a price. For Level Three securities there is no access to external data; an entity uses its own internal analysis to determine a price.

Regent Sherman requested approximate percentages for UC's Level One, Two, and Three securities. Ms. Arrivas responded that this information could be provided after the close of the fiscal year and completion of the audit. The University would have to carry this out in any case to implement the GASB standard for the next fiscal year.

Committee Chair Zettel recalled that KPMG had presented a finding to the Committee at the November 2014 meeting concerning the understatement of an asset. She asked about the risk of undervaluation of UC investments. Mr. Thomas responded that KPMG looks for valuation differences that are either high or low, and seeks to understand the processes that led to an incorrect valuation of an investment. The Office of the Chief Investment Officer had taken steps to prevent incorrect valuations. Ms. Arrivas added that UC management is required to determine the value of investments fairly soon after June 30. The external auditors have the benefit of time and are allowed to collect data through September and October. There are differences every year between these two estimates. June 2014 was a strong month overall in the markets and for the UC portfolio, and almost all the values were higher in the later valuation. The University is continuing to refine its estimation processes.

Regent Makarechian referred to the KPMG fee schedule and asked about auditing of the National Laboratories. Mr. Thomas responded that KPMG was not doing any specific separate audit work on the National Laboratories, although there are figures included in the UC financial statements related to the Laboratories. Ms. Arrivas added that the fee for the work related to the Laboratories was included in the fee for the core, consolidated audit.

Regent Sherman asked about the National Collegiate Athletic Association (NCAA) agreed-upon procedures. Mr. Thomas explained that the NCAA issues a list of procedures for colleges, by NCAA Division. The agreed-upon procedures concern revenues, expenditures, and compliance with travel and recruiting policies.

Upon motion duly made and seconded, the Committee approved the President's recommendation and voted to present it to the Board.

3. **SUMMARY OF RESULTS OF THE UNIVERSITY'S 2014 A-133 AUDIT**

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Mr. Mark Thomas of KPMG noted that the A-133 audit report was a voluminous document. The first 88 pages were financial statements the Regents had already received and approved. There followed a listing of federal awards to the UC system, approximately \$5.4 billion. Of this amount, \$1.8 billion was related to student financial aid and \$3.3 billion to funded research. The audit procedure for federal funds is very prescriptive, and the materiality threshold is very low. The report contained four findings, but these were not surprising, given the complexity of the audit and its requirements, especially in the area of student financial aid.

Regent Makarechian asked about a statement in the report according to which the University's liabilities and deferred inflows of resources decreased to \$49.2 billion in 2014. Associate Vice President and Systemwide Controller Peggy Arrivas indicated a chart listing five categories of liabilities.

Regent Makarechian requested a definition of the "expendable" category in figures for the University's net position. Ms. Arrivas responded that this referred to expendable restricted funds, funds from donors for a specific purpose.

Regent Makarechian asked if this category is counted against decreases in the University's assets. Ms. Arrivas responded that the sum of the assets and deferred outflows, minus the liabilities and deferred inflows, equals the net position. The net position is divided into categories, such as expendable or nonexpendable.

Regent Makarechian asked if the categories of "expendable" and "nonexpendable" are the same as the categories of "unrestricted" and "restricted." Ms. Arrivas responded in the negative. "Restricted" funds are those which can only be used for a particular purpose, such as debt proceeds or donor funds; "unrestricted" funds can be used for any UC purpose. She observed that UC is overdrawn in its unrestricted funds, which pay for pension and other post-employment benefit liabilities.

Referring to categories of revenues, Regent Makarechian requested clarification of the category "educational activities and auxiliary enterprises." Ms. Arrivas responded that this category includes clinical revenues received by physicians in UC schools of medicine. Auxiliary enterprises include housing, parking, dormitories, athletics, and other self-supporting activities.

Regent Makarechian asked why these clinical revenues are not included in the "medical center" revenue category. Ms. Arrivas explained that the UC medical centers receive income for their services to patients. Physicians bill separately for their services, and those revenues are recognized in the clinical revenues of the UC schools of medicine.

Regent Makarechian asked if physicians receive these monies as a salary, or if these are revenues of the University, while the physicians are on fixed contract. Ms. Arrivas responded that most UC physicians are faculty members in one of the schools of medicine, and the schools of medicine are part of their campus. The clinical revenues for physician services are school of medicine revenue rather than medical center revenue.

Regent Sherman recalled that the question of the net cost of educating a student had often been raised at meetings. He asked if the University's audit team had developed a calculation of what this cost might be. Ms. Arrivas responded in the negative. The UC financial statements are prepared under accounting principles. The audit program is not examining the cost of educating students.

Regent Sherman acknowledged that this is not part of the routinely prepared financial statements. He asked if the UC audit program could do this, to provide an independent view of that cost. Ms. Arrivas responded that this matter could be discussed in the future.

Regent Makarechian referred to a chart showing expenses associated with the Department of Energy (DOE) Laboratories. He asked if the University was receiving amounts to offset these expenses. Ms. Arrivas reported that a few weeks earlier, the University received the DOE's current-year contribution to the UC Retirement Plan (UCRP). The expenses listed in the chart were related to the Lawrence Berkeley National Laboratory; these were included in UC's financial statements, as are the expenses of the Laboratory Management Office at the Office of the President.

In response to another question by Regent Makarechian, Ms. Arrivas confirmed that the amount shown in the chart as DOE expenses might be covered partly by receivables and partly by grants.

Regent Makarechian asked if the DOE's obligation to the UCRP is treated separately. Ms. Arrivas responded that the University receives these monies separately. This obligation is included in the financial statements as an expense, because the University receives the funds from the DOE and pays them into the UCRP on the DOE's behalf. She stressed that the DOE had paid its obligation and that its current receivable was zero.

Committee Chair Zettel called attention to the fact that UC's unfunded pension liability was decreasing. The liability for retiree health benefits was also decreasing, thanks to wise investments. She asked why the University credit rating had been downgraded. Executive Vice President and Chief Financial Officer Brostrom responded that UC had gone to market the previous week with \$2.8 billion in bonds, of which \$2 billion was tax-exempt and \$800 million taxable. UC's ratings had been reaffirmed by all the rating agencies with a stable outlook. UC's general revenue credit was rated AA from Moody's, SMP, and Fitch. The rating for UC's limited project revenue bonds, used for dormitories, dining facilities, parking, and other auxiliaries, was AA-.

Committee Chair Zettel asked about KPMG letters to the campuses on findings of the audit. Ms. Arrivas responded that the letters to the chancellors were available on request. The campus responses to the findings were included in the audit report. Implementation of corrective actions was under way.

Committee Chair Zettel asked that the Regents be informed which campuses were visited after completion of the final 2015 audit. Ms. Arrivas responded that the campuses visited in 2014 and included in the current report were Berkeley, San Francisco, Davis, Los Angeles, San Diego, Santa Cruz, and Irvine.

Regent Makarechian recalled that UC general revenue bonds and limited project revenue bonds had been downgraded the previous year. Mr. Brostrom confirmed this. Committee Chair Zettel asked if the previous year's downgrade was due to an abundance of overall debt. Mr. Brostrom responded that there were several reasons for the downgrade,

including the UCRP liability, the liability for retiree health benefits, and volatility in State funding. As the State provides less of the University's overall funding, it would have a smaller impact on UC's credit ratings.

4. **USING DATA ANALYSIS TO ENHANCE AUDITING AND MONITORING ACTIVITIES**

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Systemwide Audit Director Matthew Hicks explained that data analysis was a strategic priority for UC's audit program and reflected a trend in the audit industry generally. Data analysis facilitates preliminary risk assessment and scoping to focus efforts on high risk areas. Analyzing trends in financial data year over year helps in this process. It allows for greater coverage in transactional testing. Historically, the internal audit program has used a sampling approach, drawing conclusions from a limited number of transactions. Data analysis leverages technology and is a more efficient use of auditor time. It can improve the quality and accuracy of review and helps auditors identify potential errors more efficiently. When automated, it can identify issues in real time. Data analysis helps management prepare for external audits. Governmental agencies that audit UC are increasingly using a data analysis approach. Chief Compliance and Audit Officer Vacca confirmed that this was the case with National Science Foundation audits of the University.

Data Manager Manfred Zorn elucidated how data analysis is applied to internal audit. The sampling approach has been used for a long time by auditors. Based on certain criteria, a sample of transactions is extracted. Auditors evaluate those sample transactions and extrapolate from the sample to the entire set of transactions. For example, for medical billing and coding assessments, auditors might select ten cases for each provider. The billing statements for those ten cases would be compared to the actual medical records. This process is difficult to automate. By contrast, data analysis or data analytics uses statistical methods, trending, regression analysis, or more complicated models to examine and draw conclusions about all the data. The most recent development in the arsenal of data analysis is data visualization, using visual representations of data to better understand the data and draw conclusions.

Mr. Hicks outlined one example of data analysis in the accounts payable area. Typically there is a dollar threshold for authorization of invoices. Internal audit works to identify cases where an individual may try to circumvent this internal control, one way being to break up large invoices into smaller transactions, each individually below the approval threshold. Another example of this approach would be to check for duplicate invoices. Ms. Vacca remarked on cases of fraudulent vendors, where employees have had checks sent to a post office box under a fraudulent company name.

Mr. Hicks presented another example of data analysis, a review on one campus that checked for the hiring of near relatives to identify potential policy violations. The campus

compared payroll system employee and address tables to identify any pairs of employees with the same address, and then to identify their employment funding by department or project. These pairs were the population selected for detailed testing in the audit. Another example of this approach would be comparing a vendor master file to an employee master file to identify any identical addresses, which could indicate a fictitious, fraudulent vendor.

Mr. Zorn outlined another approach in data analysis, Benford analysis. Several campuses have used Benford analysis to identify anomalies in transactional data. “Benford’s Law” was postulated in 1938 by physicist Frank Benford, and UC Berkeley Professor Emeritus Hal Varian suggested around 1970 that Benford’s Law would apply to economic and accounting transactions. According to Benford’s Law, natural number sequences follow a certain exponential pattern. Natural number sequences include population growth, credit card transactions, cash transactions, and travel expenses, as opposed to man-made sequences like zip codes. Mr. Zorn presented a chart with a “Benford curve” representing the frequency of distribution of leading digits in real-life sources of data. The first digit of cash transactions can be plotted along this curve. Deviations from the curve might indicate unusual transactions, not necessarily fraudulent, but worth examining.

Mr. Zorn then touched on data visualization. Federal agencies are using this kind of data analysis to identify unusual drawdown patterns for research awards. He presented another chart showing accumulated expenditures as trend lines, expressed as percentages of the allotted award amount. It illustrated the expenditure of awards of different sizes, from zero to 100 percent, and over time, by day, in relation to the entire allocated period. Variations from the diagonal would indicate if some award recipients spend too much of their funds in the beginning stages or at the end of a project, although this would not necessarily indicate fraud or malfeasance. Ms. Vacca noted that federal agencies are attentive to charts of this kind, looking for any anomalous patterns of spending in contracts and grants.

Mr. Hicks outlined some challenges for implementation of new technologies, such as managing change within the organization and developing internal expertise. A significant amount of upfront effort is necessary, acquiring and manipulating data, and developing scripts. It is important to select the right tools and technologies. Data availability and quality are challenges, particularly in a decentralized environment like UC, with disparate data sets. Ms. Vacca added that the internal audit program was seeking to address these challenges by training and developing subject matter experts; this would result in the need for fewer individuals to carry out manual review of transactions.

Mr. Hicks stated that goals of the internal audit program were to integrate data analysis techniques into existing audit processes and to facilitate information-sharing between campuses by forming work groups and an online collaboration forum for subject matter experts. A long-term goal of the program is to develop mechanisms for automating data acquisition. Data analysis applications would be located on servers, pulling data automatically on a daily basis and identifying exceptions and anomalies for management review.

Regent Makarechian described this process of data input, data mining, and data review as an enormous undertaking. He asked how this would be accomplished with fewer individuals. Ms. Vacca responded that the program was making use of existing data systems. She observed that some of the analytic tools did not require a great deal of manual input in order to be effective.

Regent Makarechian asked about the difficulties in bringing together data from different servers and programs. Mr. Hicks responded that currently, the internal audit program was not attempting this at a centralized, systemwide level. Campuses are performing data analysis at the local level. As the University moves toward more shared systems, there would be more opportunities to build in data analysis applications. Ms. Vacca added that UCPath would be an example of this.

Regent Sherman referred to the last, long-term goal mentioned by Mr. Hicks, developing mechanisms for automating data acquisition and analysis, and asked when it might be accomplished. Mr. Hicks responded that this was already occurring at some locations. An updated version of the data analysis tool is required.

Committee Chair Zettel underscored the potential return on investment from these data analysis methods. She asked about the software the internal audit program purchased or wished to purchase. Ms. Vacca responded that the University had already purchased software at this point; the audit program's concern was to maintain subject matter expertise in that software. Software updates represent a certain cost, but currently the audit program was able to absorb the data analysis costs in its operating budget. She expressed confidence that there would be a demonstrable return on investment as the monitoring process becomes more robust. Mr. Hicks added that cost is not usually an obstacle in implementing data analysis. Correct formatting of data and an understanding of how to use the tools are essential.

5. INTERNATIONAL ACTIVITIES REPORT

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Executive Director Elizabeth Boyd began the discussion by recalling the breadth of UC's international activities, including formal research collaborations with foreign universities, student exchanges with programs around the world, training and capacity-building efforts in underserved parts of the world, and partnerships with non-governmental organizations, foundations, and non-profit organizations. UC's global engagements are admirable but place UC within a very complex set of rules, regulations, and laws. Customs, procedures, policies, and laws vary by country and sometimes conflict with U.S. laws. The U.S. government has increased its attention and oversight and the University sometimes receives varying advice or perspectives from the U.S. government agencies involved in this area. Many regulations are new or not familiar to UC. Ms. Boyd presented a chart showing State and federal agencies involved in regulating UC's international activities.

Regent Zettel stated that it would be helpful to include U.S. agencies that affect domestic activities in this graphic.

Ms. Boyd continued by discussing the nature of federal export control laws, which govern the release or sharing of certain kinds of equipment, data, or technology with foreign collaborators, whether those collaborators are located abroad or working in the U.S. The Foreign Corrupt Practices Act prohibits payments to foreign officials for “special consideration.” The federal government’s sanctions list prohibits payments to or transactions with agents of certain foreign governments; such agents may include banks and universities. Customs regulations affect shipments into and out of the U.S. The price of misunderstanding or being found in violation of these laws and regulations is high. Federal agencies are increasingly holding academic institutions accountable for oversight. The Office of the President is taking a broad and collaborative approach in this challenging area, working across the various business units of the University.

Export Control Officer Brian Warshawsky observed that the UC systemwide export control compliance program was approaching its fourth anniversary. Historically, campus subject matter experts have resided in the research enterprise, but were now to be found in other campus units as well. Ms. Vacca underscored the fact that the establishment of a centralized export control program had been requested by the campuses.

Mr. Warshawsky stated that compliance with export control regulations involves purchasing and shipping, research, technology transfer, financial disbursement, and campus counsel. A team approach was increasingly being used to identify issues of concern, implement escalation procedures, bring in subject matter experts, ensure compliance, or take necessary action, which often concerns licensing. Ms. Vacca added that non-compliance is most often not deliberate but the result of ignorance.

There has been an increase in new sanctions issued by the U.S. government against various international parties, and Mr. Warshawsky cautioned that as the number of sanctioned parties increases, so does the likelihood that UC or other universities may inadvertently enter into a prohibited transaction with a sanctioned party or fail to determine if any of their current international collaborators have been recently sanctioned. The Office of Ethics, Compliance and Audit Services (ECAS) provides tools for screening the names of individuals and entities on sanctions lists on an ad hoc basis. ECAS is also working to develop an integrated approach for screening. An online interactive training and awareness program had been launched that week. This course is intended to prepare faculty and staff who travel abroad on UC business. Mr. Warshawsky stressed the importance of education and training; UC affiliates may not be aware that a researcher at a university in another country may qualify as a foreign official, or that a foreign university may be considered the instrumentality of a foreign government under U.S. law.

Regent Makarechian asked about control over the sending of information. Mr. Warshawsky responded that by simply sending an email message, or opening an email while abroad, an individual may be making an export or transferring technology

that others are unaware of. ECAS is working with information technology security personnel systemwide on this issue. There are no perfect solutions. He asserted that the best tool is awareness and training, for example, making people aware of the risks of traveling with a laptop computer.

Regent Ruiz acknowledged that training is crucial and asked about UC employees' accountability. Ms. Boyd responded that one step in addressing this complex problem was to bring the appropriate administrative units together to develop a comprehensive map to ensure that all relevant issues are considered when the University is contemplating an international affiliation agreement, or to ensure awareness of local laws when research projects are carried out in another country. To address the risks involved, the University must educate faculty and researchers on these issues and provide an administrative support system that can recognize when UC is entering an area of complexity where special assistance is needed.

Regent Leong Clancy asked if there was a mechanism in place to alert UC faculty, researchers, or others involved in international activities about relevant regulations and about avoiding non-compliance. Ms. Boyd responded that this would be the function of an administrative support structure. For example, there is a need in sponsored projects offices for staff who can recognize incoming projects that may raise export concerns.

Regent Makarechian asked who bears the responsibility for sending restricted data, the University or the individual. General Counsel Robinson responded that both could potentially be considered responsible for violations.

Regent Makarechian observed that the University would then be required to indemnify the individual. Mr. Robinson confirmed this. Regent Makarechian stressed the importance of education and awareness. UC researchers must be aware of potential sizeable penalties. Mr. Robinson responded with his view that most UC researchers have good intentions. It was a matter of training and educating them. The University should identify areas where it faces the greatest risk and where the federal government would have the greatest concern. UC should begin its efforts in those areas.

6. ETHICS AND COMPLIANCE ACTIVITIES REPORT

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Chief Compliance and Audit Officer Vacca suggested that discussion of this item be deferred until the next meeting, due to time constraints.

7. INTERNAL AUDIT ACTIVITIES REPORT

[Background material was provided to Regents in advance of the meeting, and a copy is on file in the Office of the Secretary and Chief of Staff.]

Systemwide Audit Director Matthew Hicks referred to concerns expressed earlier by Regent Makarechian about construction risk. He noted that this is an area of focus for the internal audit program. The Office of Ethics, Compliance and Audit Services has asked each campus to include at least one construction project in its audit plan. Typically, campuses review the competitive bid process, including compliance requirements for change orders.

Systemwide Information Technology Audit Manager Greg Loge discussed information technology risk and how the internal audit program was addressing it. The risk of data breaches was on the rise, as demonstrated by hacking events during the past year. Many breaches have been due to increased hacking activity and more sophisticated attacks using malicious software. Healthcare entities and patient data are increasingly a target for hackers. The higher education environment poses unique security challenges due to its relatively open and distributed information technology systems.

The Ponemon Institute carries out an annual study of the cost of data breaches. In the most recent study, the Institute reported that the average breach resulted in slightly more than 29,000 records being exposed. The Institute also calculated the cost per record to an entity. In the U.S., this is on average approximately \$200 per record, resulting in an average cost per breach of over \$5 million over a two-year period. Mr. Loge underscored that the two industries with the highest breach costs are health care and education.

A number of factors influence the cost of breaches. Loss or theft of devices is an important factor, and this accounted for many healthcare data breaches over the past year. A strong security posture is one important way of reducing the cost of a breach. The open and distributed networks in higher education make it harder to achieve a strong security posture in this environment, compared to other industries. The Ponemon Institute study also examined the root causes of breaches. Approximately 40 percent of breaches were caused by malicious or criminal acts, about 30 percent by human error, and 30 percent by system glitches.

Another noteworthy study was conducted by Educause, a leading information technology research organization in higher education. In this study of incidents between 2005 and 2014, the largest segment of reported breaches in higher education was related to malware and hacking, as well as unintended disclosure. Chief Compliance and Audit Officer Vacca recalled that a sophisticated hacking intrusion into the system had occurred at UC Berkeley a few years earlier, with significant costs to the campus.

Mr. Loge continued, referring to one of the most comprehensive data breach studies, carried out annually by Verizon. Data for this study are compiled from more than 40 contributing organizations, including law enforcement, higher education, and healthcare institutions. According to the Verizon report, incidents at educational institutions were mostly due to web application attacks, physical theft and loss, and miscellaneous errors. In healthcare institutions, physical theft and loss accounted for 46 percent of incidents, while insider misuse was the cause of 15 percent of incidents.

UC's internal audit program reviews research and studies like the three mentioned to determine key areas of risk.

One such area is web application attacks. Based on industry research, certain controls are recommended to reduce this risk: stronger alternatives to single passwords, using multi-factor authentication; input validation, ascertaining that what is being typed into web applications does not include code that could be used to compromise systems; enforcing lockout policies to prevent brute force attacks, such as attempts to gain access to a system by guessing passwords over and over again; and monitoring outbound connections, examining data leaving the web application for anomalies.

Physical theft and loss are other significant areas of risk for both healthcare and higher education entities. The most frequent locations for theft identified in the Verizon study are first the victim work area, second, the personal vehicle, and third, the personal residence. Recommended controls to reduce this risk are encryption of devices, data backups to allow quick recovery from loss of information, locking down equipment, and keeping equipment with the individual. Ms. Vacca noted that outdated equipment with data is sometimes forgotten. In one recent case, older computers left in a locked area were stolen.

Mr. Loge then outlined how the internal audit program was addressing these risks. The program was staying apprised of industry risks and best practices, to align its focus and determine which audits to perform. It was leveraging a recognized industry framework for information security, a framework which is accepted in the UC information technology community. Within its own organization, the internal audit program was seeking to identify competencies for the risk areas discussed, and to train staff for these areas. At this time, the program was working through the annual risk assessment process, identifying areas of focus for campus audits in the next fiscal year. Coordinated audit projects would address issues that arise across campuses.

Committee Chair Zettel emphasized the importance of these efforts. As the University seeks to work more efficiently, the cost of even a single data breach can eliminate gains made by those efficiencies. She expressed concern that some campuses may be many years behind in employees' knowledge of best practices in privacy protection.

Regent Makarechian referred to information from the Educause study. He requested a definition of the term "unintended disclosure." Mr. Loge responded that there have been examples of sensitive information put on web servers, intended to be accessible for only a certain group of individuals in a department, but configured in such a way that individuals from outside the University could have access to it. He recalled that the Educause data reflected a ten-year trend; at the current time it was possible that cases of unintended disclosure were on the decrease. He noted that in the past, student Social Security numbers were used as identifiers, for example on spreadsheets with student grades, and this kind of information might be disclosed unintentionally.

Regent Makarechian asked how this problem can be addressed. Mr. Loge responded that this issue should be raised in reviewing the organization of information technology at UC and information security practices. The internal audit program would work with departments to ensure that they have a good understanding about the locations of sensitive data and how data are secured. Past incidents were sometimes the result of employees not knowing where all the sensitive data were located, or who was storing which data, and in which location.

Regent Makarechian asked about responsibility in this area. Mr. Loge responded that it is the responsibility of management. The internal audit program performs reviews to see if work is being done appropriately, but internal audit does not carry out this work. Ms. Vacca added that campuses no longer use Social Security numbers unless necessary and protect these data.

Regent Leong Clancy asked if current best practices favor cloud storage for data, rather than keeping data on a laptop computer or other device that can be removed. Mr. Loge responded that there was currently a trend to move more data to the cloud, in part motivated by cost savings. Cloud storage also introduces some risks and changes how the University addresses those risks. If an audit identifies an outside vendor that relies heavily on cloud services, it would consider other types of controls, the contracts UC has with that organization, and the expectations UC has for data secured by that organization, the organization's attestations, and UC's risk. The move to cloud computing was positive in many ways, but introduced a new risk profile.

The meeting adjourned at 1:05 p.m.

Attest:

Secretary and Chief of Staff



cutting through complexity

University of California Audit Plan June 30, 2015

March 2015



Mark Thomas
National Client Leader,
Higher Education Practice

mtthomas@kpmg.com
714-809-0190

February 6, 2015

University of California

Members of the Committee on Compliance and Audit:

We are pleased to present for your review the Audit Plan for the 2014/2015 audits of the University of California. The objective of our audit planning activities is to prepare for an effective audit. As a part of that process and in accordance with auditing standards, we are communicating with you certain matters related to the planned conduct of the audits.

Included in this Audit Plan are overviews of the following topics:

- **Our audit objectives**
- **Planned deliverables**
- **KPMG's client service team leaders**
- **Planned timeline**
- **The responsibilities of KPMG, management, and the Board**
- **Identification of audit risk areas**
- **A discussion of materiality**
- **Confirmation of KPMG's independence**
- **A summary of fees.**

I look forward to seeing you at your meeting in March, and will be available to answer any questions you may have.

Best Regards,

Mark Thomas

Lead Engagement Partner

Contents

- 1 Audit Objectives**
- 2. Deliverables**
- 3. Client Service Team**
- 4. Timeline**
- 5. Responsibilities**
- 6. Risk Assessment**
- 7. Audit Plan - Materiality**
- 8 Independence**
- 9 Fees**

Audit Objectives

Objectives:

- We plan and will perform the audits to obtain reasonable assurance about whether the financial statements taken as a whole are free from material misstatement, whether from error or fraud.

- Our audit includes:
 - Performing tests of the accounting records and such other procedures, as we consider necessary in the circumstances, based on our judgment, including the assessment of the risks of material misstatement to provide a reasonable basis for our opinions.
 - Evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, and evaluating the overall financial statement presentation.

The objective of our audits of the financial statements is to enable KPMG to express opinions about whether the financial statements (prepared by management with the oversight of the Audit Committee) are presented fairly, in all material respects, in conformity with generally accepted accounting principles (GAAP).

Deliverables

Financial Statement Audit Opinions

- **University of California Systemwide Financial Statements**
- **Each of the 5 University Medical Centers**
- **University of California Retirement System**
- **University Captive Insurance Company**

Additional Reports

- **Single Audit of Federal Funds expended in accordance with OMB Circular A-133**
- **Report on the University of California Cash Contributions to the Retirement System**
- **Agreed-upon procedures related to the Mortgage Origination Loan Program**
- **Agreed-upon procedures related to NCAA requirements (6 campuses)**
- **Agreed-upon procedures related to Student Health Insurance Program**

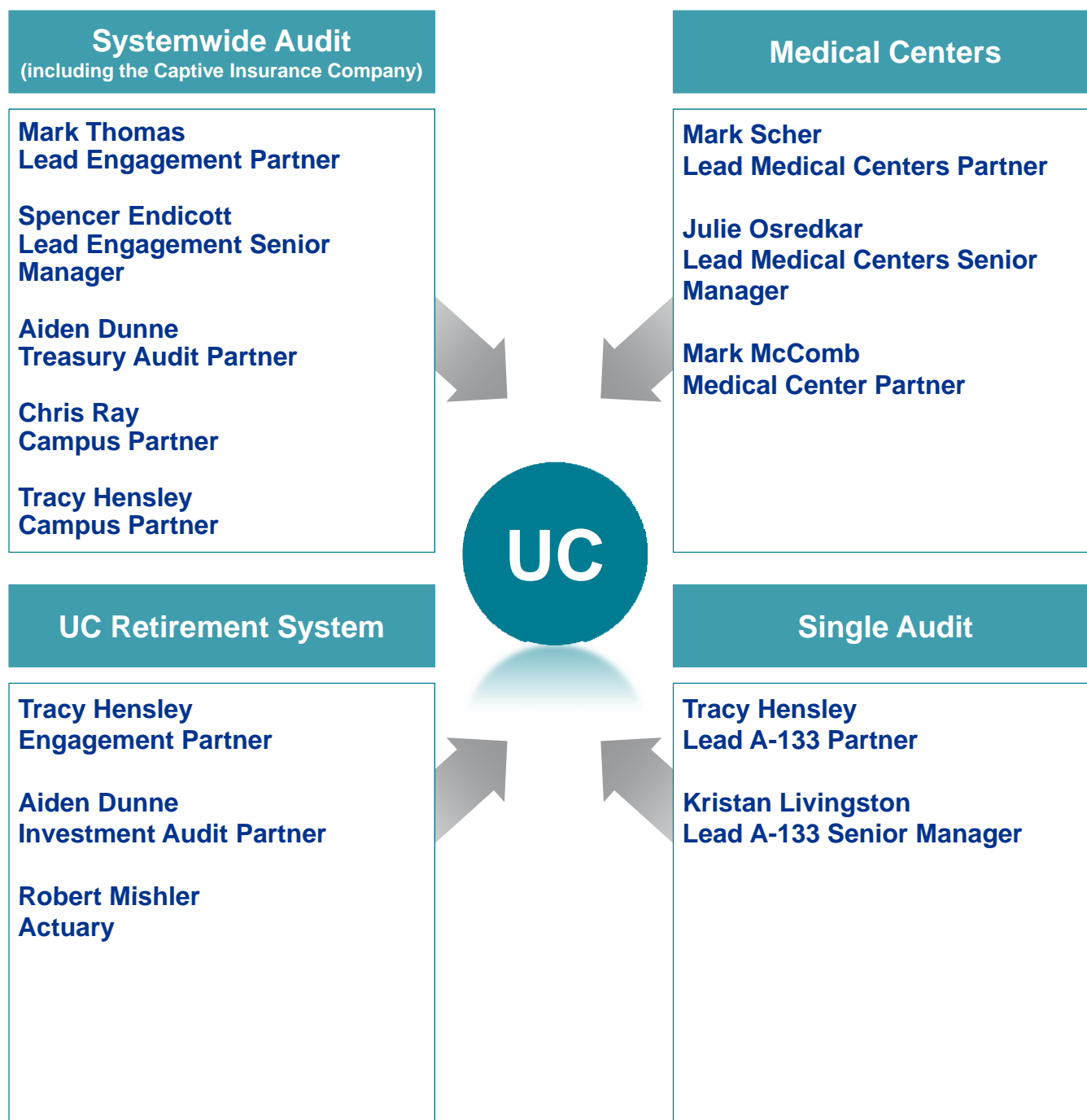
Internal Controls

- **Letter to Regents on internal control deficiencies that are considered Significant Deficiencies and/or Material Weaknesses**

Required Communications

- **Audit Plan**
- **Audit results and required communications relating to the conduct of the audit**

Client Service Team



Timeline

Planning, risk assessments, set scopes by location	January - March
Present overall Audit Plan to the Audit Committee	March
Information Technology Testwork	March - June
Interim fieldwork	April – June
Final fieldwork	August – October
Issue financial statement audit reports	October
Present financial statement audit results to the Audit Committee	November
Complete additional reports and procedures, including Single Audit	November - January

Responsibilities

Management is responsible for:

- Adopting sound accounting policies
- Fairly presenting the financial statements in conformity with GAAP
- Establishing and maintaining effective internal control over financial reporting (ICFR)
- Identifying and confirming that the University complies with laws and regulations applicable to its activities
- Making all financial records and related information available to the auditor
- Providing unrestricted access to person's within the entity from whom the auditor determines it necessary to obtain audit evidence
- Providing the auditor with a letter confirming certain representations made during the audit that include, but are not limited to, management's:
 - Disclosure of all significant deficiencies, including material weaknesses, in the design or operation of ICFR that could adversely affect the University's ability to initiate, authorize, record, process, or report financial data
 - Acknowledgement of their responsibility for the design and implementation of programs and controls to prevent, deter, and detect fraud
 - Responsibility for adjusting the financial statements to correct material misstatements relating to accounts or disclosures and for affirming to the auditor in the representation letter that the effects of any uncorrected misstatements aggregated by the auditor are immaterial, both individually and in the aggregate, to the financial statements taken as a whole.

Responsibilities (continued)

The Audit Committee is responsible for:

- Oversight of the financial reporting process and oversight of internal control over financial reporting (ICFR)
- Oversight of the establishment and maintenance by management of programs and internal controls designed to prevent and detect fraud

Management and the Audit Committee are responsible for:

- Setting the proper tone and creating and maintaining a culture of honesty and high ethical standards

Responsibilities (continued)

KPMG is responsible for:

- Forming and expressing an opinion about whether the financial statements (that have been prepared by management, with the oversight of those charged with governance), are prepared, in all material respects, in accordance with the applicable financial reporting framework
- Planning and performing the audit with an attitude of professional skepticism
- Conducting the audit in accordance with professional standards and complying with the Code of Professional Conduct of the American Institute of Certified Public Accountants, and the ethical standards of the California CPA societies and California State Board of Accountancy
- Evaluating internal controls over financial reporting (ICFR) as a basis for designing audit procedures, but not for the purpose of expressing an opinion on the effectiveness of the entity's ICFR
- Communicating to management and the Audit Committee all required information, including significant matters
- Communicating to the Audit Committee and management in writing all significant deficiencies and material weaknesses in internal control identified in the audit and reporting to management all deficiencies noted during our audit that are of sufficient importance to merit management's attention

Risk Assessments

Significant audit areas	Significant estimates	Significant unusual transactions/other items
■ Investments	■ Determination of fair values	■ Complex and hard to value alternative investments
■ Medical Center revenue recognition	■ Contractual allowances and bad debts	■ Significant complexity in calculating contractual and bad debt allowances
■ Pension and postretirement obligations	■ Actuarial assumptions drive liability estimates	■ Implementation of new accounting pronouncements in the current year
■ Long-term debt	■ Calculation of economic gain/loss on refunding transactions	■ Refunding of debt in the current fiscal year
■ Grants and contracts	■ Significant compliance requirements attach to these revenues	■ Expenditures will be subject to audit procedures required by OMB Circular A-133
■ IT implementations	■ Significant implementations occurring throughout the System	■ Involve KPMG IT Specialists to evaluate critical systems that drive financial reporting

Audit Plan – Materiality

- Professional standards require that we exercise professional judgment when we consider materiality and its relationship with audit risk when determining the nature, timing, and extent of our audit procedures, and when evaluating the effect of misstatements.
- Information is material if its omission or misstatement could influence the economic decisions of users taken on the basis of the financial statements.
- Materiality depends on the size and nature of the item or error judged in the particular circumstances of its omission or misstatement.
- Judgments about matters that are material to users of the financial statements are based on a consideration of the common financial information needs of users as a group. The possible effect of misstatements on specific individual users, whose needs may vary widely, is not considered.

Independence

As your auditor, KPMG is subject to the independence standards imposed by the American Institute of Certified Public Accountants (AICPA), Code of Professional Ethics, the standards of independence established by Government Auditing Standards, published by the United States General Accounting Office (GAO), as well as the rules of the California State Board of Accountancy. We fully subscribe to those standards. We confirm that we, are “independent” of the University of California and its component units, as defined by the aforementioned standards.

Fees

UC Entity/Report	2015 Fees
UC Consolidated Entity	\$ 1,370,250
Single Audit (A-133 Audit)	393,900
Medical Center Audits	1,096,470
University of California Retirement System Audits	152,300
NCAA Agreed-Upon Procedures	85,925
Mortgage Origination Program Agreed-Upon Procedures	9,280
UC Captive Insurance Company Audit	28,600
UC Retirement Plan's Schedule of Cash Contributions	4,910
UCLA Medical Center Bond Opinion	2,455
Consolidated Form 990T Review	15,200
Total	\$ 3,159,290



cutting through complexity

© 2015 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 203783

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.