AGENDA

COMMITTEE ON AUDIT

Meeting: **4:45 p.m., Tuesday, July 10, 2007**
Glenn S. Dumke Auditorium

8:45 a.m., Wednesday, July 11, 2007
Glenn S. Dumke Auditorium

Raymond W. Holdsworth, Chair
Kenneth Fong, Vice Chair
Herbert L. Carter
George G. Gowgani
Melinda Guzman
William Hauck
Ricardo Icaza
Glen O. Toney

4:45 p.m., Tuesday, July 10, 2007 -- Glenn S. Dumke Auditorium

Consent Items

Approval of Minutes of Meeting of May 16, 2007

Discussion Items

1. Status Report on Current and Follow-up Internal Audit Assignments, *Information*
2. California State University Information Security Program Status Report, *Information*

*****NOTE***

8:45 a.m., Wednesday, July 11, 2007 -- Glenn S. Dumke Auditorium

Consent Items

Approval of Minutes of Meeting of May 16, 2007

Discussion Items

1. Status Report on Current and Follow-up Internal Audit Assignments, *Information*
2. California State University Information Security Program Status Report, *Information*

****NOTE:** *Depending on the length of discussion on Tuesday, July 10, 2007, Committee on Audit items may have to be carried over to Wednesday, July 11, 2007 for consideration.*

MINUTES OF THE MEETING OF
COMMITTEE ON AUDIT

Trustees of The California State University
Office of the Chancellor
Glenn S. Dumke Conference Center
401 Golden Shore
Long Beach, California

May 16, 2007

Members Present

Raymond W. Holdsworth, Chair
Debra S. Farar, Vice Chair
Roberta Achtenberg, Chair of the Board
Herbert L. Carter
Carol R. Chandler
George G. Gowgani
William Hauck
Glen O. Toney

Chair Holdsworth called the meeting to order.

Approval of Minutes

The minutes of the meeting of March 13, 2007, were approved as submitted.

Status Report on Current and Follow-up Internal Audit Assignments

Mr. Larry Mandel, university auditor, presented the Status Report on Current and Follow-up Internal Audit Assignments, Agenda Item 1 of the May 15-16, 2007, Board of Trustees agenda.

Mr. Mandel indicated that the campuses continue to make exceedingly good progress in the timely completion of the recommendations, and commented that their efforts resulted in the most complete status report ever presented to the Trustees. He reported that since the Agenda Book mail-out, there had been approximately 15 updates to the status report regarding the completion of the outstanding recommendations. Mr. Mandel noted that only two areas have been outstanding for several months (Continuing Education, Systemwide and Housing and Residential Services, Systemwide). He stated that the three recommendations for Housing and Residential Services pertained to Title V changes, and have essentially been completed.

Chair Holdsworth inquired about the timeline for completion of the outstanding systemwide recommendations pertaining to Continuing Education.

Mr. Richard P. West, executive vice chancellor and chief financial officer, stated that the delay in the completion of the recommendations for Continuing Education was due to the inception of the Revenue Management Program, which caused the necessary review of accounting practices in this area. He anticipated completion of the outstanding recommendations for Continuing Education by September 2007.

Chair Holdsworth also remarked on the progress that has been made on the status report in completing the recommendations in a timely manner. He thanked the presidents and their staffs for the considerable attention and effort given in this accomplishment.

Trustee Carter inquired about the outstanding recommendations pertaining to Disaster and Emergency Preparedness for the chancellor's office.

Mr. Mandel stated that it has only been three months since the exit conference meeting where the preliminary draft report pertaining to Disaster and Emergency Preparedness was discussed with the chancellor's office. He explained that supporting documentation is typically received from the campus or chancellor's office over a longer period of time.

Chair Holdsworth discussed the upcoming financial statement audit for fiscal year ending June 30, 2007. He addressed the presidents, stating that they should discuss any staffing issues or concerns with their vice presidents to determine if any assistance is needed from the chancellor's office in order to ensure a timely completion. He advised the presidents to review the recommendations from last year's financial statement audit to use as a guide in preparation of the upcoming audit. Chair Holdsworth discussed the schedule for the completion of the financial statement preparation process and provided the following due dates:

- Auxiliary organizations – end of September 2007
- Campuses – October 18, 2007
- Systemwide reporting – mid-December

COMMITTEE ON AUDIT

Status Report on Current and Follow-up Internal Audit Assignments

Presentation By

Larry Mandel
University Auditor

Summary

This item includes both a status report on the 2007 audit plan and follow-up on past assignments. For the current year, assignments have been made to conduct reviews of FISMA (financial internal controls), Auxiliary Organizations, Contracts and Grants, Occupational Health and Safety, Athletics Administration, and Construction. In addition, follow-up on past assignments (FISMA, Auxiliary Organizations, Continuing Education, Housing and Residential Services, Delegations of Authority, Disaster and Emergency Preparedness, and Athletics Administration) is currently being conducted on approximately 30 prior campus/auxiliary reviews. Attachment A summarizes the reviews in tabular form. An up-to-date Attachment A will be distributed at the Committee meeting.

Status Report on Current and Follow-up Internal Audit Assignments

At the January 2007 meeting of the Committee on Audit, an audit plan calling for the review of the following subject areas was approved: FISMA (financial internal controls), Auxiliary Organizations, Contracts and Grants, Occupational Health and Safety, Athletics Administration, and Construction.

FISMA

The initial audit plan indicated that approximately 130 staff weeks of activity (15 percent of the plan) would be devoted to auditing financial internal controls on 12 campuses. Two audits await a campus response prior to finalization, and report writing is being completed on three campuses.

Auxiliary Organizations

The initial audit plan indicated that approximately 286 staff weeks of activity (34 percent of the plan) would be devoted to auditing internal compliance/internal control at 8 campuses/29 auxiliaries. Report writing is being completed at four campuses/fourteen auxiliaries.

Contracts and Grants

The initial audit plan indicated that approximately 97 staff weeks of activity (11 percent of the plan) would be devoted to a review of 10 campuses on solicitation activities and project approval; contract/grant budgeting and financial planning; cost accounting, allocation, and transfer processes; and award administration. Report writing is being completed at two campuses, while fieldwork is currently taking place at one campus.

Occupational Health and Safety

The initial audit plan indicated that approximately 97 staff weeks of activity (11 percent of the plan) would be devoted to oversight of the campus injury and illness prevention program (IIPP), job and workplace conditions, employee health examinations and medical monitoring, health and safety training, work-related accidents, and programs for complying with federal and state occupational regulations. Report writing is being completed at one campus, while fieldwork is currently taking place at two campuses.

Athletics Administration

The initial audit plan indicated that approximately 79 staff weeks of activity (9 percent of the audit plan) would be devoted to a review of five to seven campuses to ensure proper administration/review of the general control environment for athletics and control activities undertaken to assure implementation of appropriate institutional systems, policies and procedures for financial oversight, and stewardship of athletics. Report writing is being completed at two campuses, while fieldwork is currently taking place at two campuses.

Information Systems

The initial audit plan indicated that approximately 45 staff weeks of activity (5 percent of the plan) would be devoted to review of systemwide projects such as: Disaster Recovery, Common Management Systems (CMS), and Web Security. In addition, support will be provided in the area of financial internal controls for both campus (FISMA) and auxiliary audits. Review and training are ongoing.

Follow-ups

The audit plan indicated that approximately 26 staff weeks of activity (3 percent of the plan) would be devoted to follow-up on prior audit recommendations. The Office of the University Auditor is currently tracking approximately 30 prior audits (FISMA, Auxiliary Organizations, Continuing Education, Housing and Residential Services, Delegations of Authority, Disaster and Emergency Preparedness, and Athletics Administration) to determine the appropriateness of the corrective action taken for each recommendation and whether additional action is required.

Consultations

The Office of the University Auditor is periodically called upon to provide consultation to the campuses and/or to perform special audit requests made by the Chancellor. Thirty-eight staff weeks have been set aside for this purpose, representing approximately 4 percent of the audit plan.

Investigations

The Office of the University Auditor is periodically called upon to provide investigative reviews which are often the result of alleged defalcations or conflicts of interest. In addition, whistleblower investigations are being performed on an ongoing basis, both by referral from the State Auditor, and directly from the chancellor's office. Forty-five staff weeks have been set aside for this purpose, representing approximately 5 percent of the audit plan.

Construction

The audit plan indicated that approximately five staff weeks of activity (1 percent of the plan) would be devoted to coordination of construction auditing. For the 2006/07 fiscal year, six construction projects are being reviewed by KPMG with coordination from the Office of the University Auditor. Areas under review include construction bid process, change orders, project management services, contractor compliance, liquidated damages, and cost verification of major equipment and construction components. Five staff weeks have been set aside for this purpose, representing approximately 1 percent of the audit plan. Three audits await responses from the campuses/chancellor's office prior to finalization, and report writing is currently being completed on three projects.

Status Report on Current and Follow-Up Internal Audit Assignments
(as of 7/9/2007)

	2007 ASSIGNMENTS					FOLLOW-UP ON PAST/CURRENT ASSIGNMENTS															
	FISMA	Aux Orgs	Contracts and Grants	Occ Hlth and Safety	Athletics Admin	FISMA		Auxiliary Organizations			Continuing Education		Housing & Res Svcs		Del of Authority		Dis & Emerg Preparedness		Athletics Administration	
						*Recs	**Mo.	•No.	*Recs	**Mo.	*Recs	**Mo.	*Recs	**Mo.	*Recs	**Mo.	*Recs	**Mo.	*Recs	**Mo.
BAK					FW	12/12	-	3	22/22	-					7/7	-				
CHI			FW			7/7	-	3	0/6	3	9/9	-								
CI						13/13	-	2	26/26	-							7/7	-		
DH	RW							3	5/14	3							9/9	-		
EB				RW		16/16	-	4	40/40	-										
FRE			RW			7/7	-	6	47/47	-							3/3	-	0/15	2
FUL						7/7	-	4	31/31	-	5/5	-							6/9	4
HUM					FW	0/14	3	3	25/25	-							4/7	6		
LB					RW	13/13	-	3	19/19	-	5/5	-	10/10	-	4/4	-				
LA						5/5	-	4	42/42	-	2/2	-			7/7	-				
MA						0/16	3	2	14/14	-	12/12	-								
MB				FW		8/8	-	2	17/17	-					5/10	5				
NOR					RW	8/8	-	5	26/30	4			9/9	-						
POM		RW				6/10	5	3			7/7	-	11/11	-			4/4	-		
SAC			RW			0/10	2	5	36/36	-									13/13	-
SB	RW							3	17/17	-							6/6	-		
SD	AI	RW						4					10/10	-			6/6	-	6/14	4
SF	AI			FW				4	32/32	-			7/7	-	4/4	-				
SJ		RW				0/24	2	4		-					6/6	-			9/20	5
SLO						10/10	-	2	13/13	-			4/4	-						
SM		RW				11/11	-	3			5/5	-			7/7	-				
SON						6/6	-	4	17/18	4			10/10	-			5/5	-		
STA	RW							4	27/27	-					7/7	-				
CO						4/4	-	2	11/11	-					9/9	-	5/8	5		
SYS											3/6	13	8/8	-	7/7	-				

FW = Field Work In Progress
RW = Report Writing in Progress
AI = Audit Incomplete (awaiting formal exit conference and/or campus response)
AC = Audit Complete

* The number of recommendations satisfactorily addressed followed by the number of recommendations in the original report.
A "0" in a column is used as a place holder until such time as documentation is provided to the OUA evidencing that a recommendation has been satisfactorily addressed; significant progress may have been made prior to that time.
Numbers/letters in red are updates since the agenda mailout.
**The number of months recommendations have been outstanding (since the formal campus exit conference).
• The number of auxiliary organizations reviewed.

Status Report on Current and Follow-Up Construction Audit Assignments
(as of 7/9/2007)

	Project	Project	Contractor	Construction	Start	Comp.	Managed	Current	Campus Follow-Up		CPDC Follow-Up	
	No.			Cost	Date	Date	By	*	**RECS	***MO.	**RECS	***MO.
2006/07	EB-51	Pioneer Hts Stdt Hsg Ph II	C Overaa & Co.	$25,020,000	3/7/2005	Jul-06	Campus	AI				
	SD-652	Social Science/Pkg Str 8	douglas e. barnhart	$23,749,618	6/1/2004	Oct-06	Campus	AI				
	SO-410	Renovate Darwin Hall	Rudolph & Sletten	$22,471,000	2/14/2005	Jul-06	Campus	RW				
	SB-304	SCI Bldg Annex Ph II	Kemp Bros Constr	$19,695,000	7/7/2003	Jan-06	Campus	RW				
	EB-236	Valley Bus & Tech Bldg	Flintco, Inc.	$18,870,000	3/15/2005	Jul-06	Campus	AI				
	SF-570	Renovate Hensil Hall	Pacific Engrs/Swinerton	$15,398,691	6/23/2000	Sep-05	Campus	RW				
2005/06	SJ-703	Campus Village Apartments	Clark Construction	$161,431,000	12/9/2002	Aug-05	Campus	AC	10.5/10.5	-	1.5/1.5	-
	MB-777	No. Quad Student Housing	Webcor Builders	$36,405,503	1/27/2003	Sep-04	Campus	AC	5.5/5.5	-	1.5/1.5	-
	FU-695	Auditorium/Fine Arts Ph II	Hensel Phelps	$35,978,000	11/1/2003	Jan-06	Campus	AC	4/4	-	1/1	-
	PO-31	University Village, Ph III	Multiple Primes	$22,605,000	11/1/2003	Sep-05	Campus	AC	3/3	-	1/1	-
	SM-631	Academic Hall Bldg 13 (Bus)	CE Wylie Construction	$20,500,000	5/22/2004	Dec-05	Campus	AC	4.5/4.5	-	0.5/0.5	-
	FR-231	Sci II Replacement Building	LC Nelson & Sons	$16,822,000	8/4/2003	May-05	Campus	AC	12/12	-	-	-
	*FW = Field Work in Progress; RW = Report Writing in Progress; AI = Audit Incomplete (awaiting response); AC = Audit Complete											
	**The number of recommendations satisfactorily addressed followed by the number of recommedations in the original report.											
	***The number of months that recommendations have been outstanding (since the formal exit conference).											

COMMITTEE ON AUDIT

California State University Information Security Program Status Report

Presentation By

David Ernst
Assistant Vice Chancellor
Information Technology Services

Background

The issue of information security is a major concern to the CSU. In early 2004, the California State University engaged a consultant to do an overview of information security within the CSU. The consulting study identified deficiencies at both campus and system levels, and recommended three major corrective actions:

- Hire an Information Security Director to lead systemwide efforts to raise information security awareness and oversee information security management for the University
- Develop a systemwide information security plan and move rapidly to implement it
- Require every campus to designate an individual with campus-wide responsibility and authority for information security

CSU has acted on these recommendations and hired a professional Information Security Officer for the system, made technical improvements to systems as appropriate and begun the development of security plans, policies and standards. In addition, campuses have each designated a person responsible for information security, and presidents have discussed the issue in depth at the last three Executive Council retreats. We reported on this progress to the Committee on Audit in November 2006. The development of a comprehensive systemwide security plan is underway. There are two critical components of that plan, which we highlight for the Trustees here:

- Systemwide Policies and Standards
- Security Awareness and Training

Systemwide Security Plan

One of the objectives of the systemwide security plan project is to create a blueprint for the development of the CSU information security program. The security plan will include the security gap analysis that describes variances between existing processes (i.e., risk assessment, business impact analysis, security policies/standards/procedures, authorization and access control

etc.,) and information security best practices. Also included will be review and assessment of CSU's processes to determine risks and exposures and to identify security deficiencies faced by the University.

Early in the process, the University decided to use industry standards as the benchmark for its security practices. In order to expedite implementation of a plan, and due to limited staffing in this area, we decide to use professional experts to guide both our analysis and plan development and implementation.

Gap Analysis

In mid-2006, Unisys was awarded a contract to assist the CSU in the systemwide security plan project. A high-level information security survey of nine (9) campuses and the Chancellor's Office was conducted. The campuses selected to participate in this survey included:

- *3 large campuses*
  - Long Beach
  - Northridge
  - San Francisco
- *3 medium campuses*
  - San Luis Obispo
  - East Bay
  - Fresno
- *3 small campuses*
  - San Marcos
  - Sonoma
  - Stanislaus

Selected sites were assessed against an industry information security standard, ISO 17799:2005, Code of Practice for Information Security Program Management, as well as currently applicable industry regulations and State and Federal laws. This assessment was not an audit, but a snapshot of the state of information security as benchmarked against these industry information security standards. The scope of this project was to determine the risks, exposures and controls of existing practices and processes. (For a complete listing of areas benchmarked, see Attachment A.) The Unisys assessment was completed in June 2007.

Gap Analysis Conclusions

Several areas that need attention on a systemwide basis were identified:

1. Develop Information Security Policies and Standards

Recommendation: The CSU should develop a minimum set of systemwide policies and standards that establish boundaries within which to operate, but will also allow campuses a degree of autonomy in how they meet the policy requirements.

2. Security Awareness and Training

Recommendation: The CSU should develop a security awareness and training program for all employees, contractors and students. Various regulatory and statutory requirements obligate the CSU to provide appropriate training to individuals who are granted access to confidential, sensitive and proprietary information.

3. Organizational Information Security

Recommendation: The CSU should establish a governance model for the information system program. This model should also define roles and responsibilities, identify stakeholders, and recommend staffing models for supporting the information security functions at the campuses and the Chancellor's office. Campuses are encouraged to look at their organizations to determine the best approach for integrating information security into their existing governance structure.

4. Data and Asset Classification

Recommendation: The CSU should develop a system of data and asset classification that includes guidance on handling procedures for each of the levels of data identified.

5. Incident Management

Recommendation: The CSU should develop a plan to manage information security related incidents. The CSU incident response policy should include the definition of what is an event versus an incident. Reporting procedures should be clearly documented. Procedures for collecting evidence should be established.

6. Business Continuity/Resumption Planning

Recommendation: Executive Order 921 requires that campuses and the Office of the Chancellor develop business continuity plans. CSU should launch an initiative to assist campuses in the review and update of their plans to ensure compliance with information security policy and best practice.

The CSU Information Security Plan will describe the closing of the gaps identified by the Unisys review as well as the longer term efforts necessary to build information security into the culture of the CSU. It will also lay out the transition from information security projects to an on-going information security program. The draft plan will be ready for general review this fall.

Currently, campuses and the Chancellor's Office are working collaboratively on addressing the findings from the systemwide gap analysis report. They are also addressing systemwide policies, performance measures and targeted information security oriented training programs.

Systemwide Security Policies and Standards

The CSU will be engaging a consulting firm to help develop systemwide policies and standards. We expect to award the contract in late July 2007 with engagement completion expected in Spring 2008. In addition to the development of systemwide policies and standards, the selected contractor also will help the campuses with implementation of the new policies and standards. Campuses will develop local procedures to comply with the systemwide policies; and to ensure there is a process to verify that compliance.

Systemwide Security Awareness and Training

The CSU plans to engage consulting assistance to help develop and provide web-based security awareness training to all staff, including auxiliary organizations. The development of the request for proposals has just begun and the expected engagement completion is not yet determined. This training also will be made available to contractors and vendors who are granted access to CSU information assets.

Conclusion

Maximizing information security protection requires focus and coordination among people, processes and technology improvements. To achieve a targeted state of information assurance, at a minimum, CSU must:

- Develop an effective information security protection program that aligns with management's strategic objectives

- Promote a security aware culture through communication and training programs
- Develop policies, standards and good business practices that are designed to ensure the confidentiality, integrity and availability of CSU information assets

Establishing an effective security program typically takes three to five years in large organizations. Maintaining senior management commitment and investment for the duration of the project is essential. Carefully choosing a combination of both short-term, "quick hit" projects that emphasize value and longer-term infrastructural and cultural change projects will provide incremental increases in program quality while strengthening management support.

Beginning in 2008, the University Auditor will begin auditing campus compliance with security best practices and closing the gaps identified in the consultants report.

ATTACHMENT A – Domains Reviewed During the Unisys Assessment

ISO 17799:2005 Information Technology – Code of Practice for Information Security Management

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Regulatory and Statutory Regulations

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- California's SB 1386
- Payment Credit Industry Standard (PCI)
- Digital Millennium Copyright Act (DMCA)