UCSB Audit and Advisory Services

Internal Audit Report

Student Information System (SIS) Modernization Project
Limited Scope Progress Review

July 1, 2014

Performed by:
Antonio Manas-Melendez, Senior Auditor

Approved by:
Robert Tarsia, Director

Report No. 08-14-0007

This page intentionally left blank.

University of California, Santa Barbara

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
SANTA BARBARA, CALIFORNIA 93106-5140
Tel: (805) 893-2829
Fax: (805) 893-5423

July 1, 2014

To: Bill McTague
Executive Director of Resource Planning, IT, and Sustainability
Student Affairs

Lubomir Bojilov
Executive Director & CTO, Student Information Systems & Technology

Re: **Student Information Systems (SIS) Modernization Project**
Limited Scope Progress Review
Audit Report No. 08-14-0007

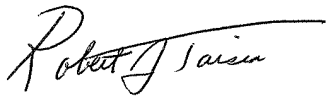
As part of the 2013-14 annual audit services plan, Audit and Advisory Services has completed a limited scope progress review of the University of California, Santa Barbara (UCSB) Student Information System (SIS) Modernization Project. Enclosed is the report detailing the results of our review.

The purpose of this audit included a review of selected areas relevant to the project from February 2013 to February 2014, as well as follow-up of related issues from a fiscal year 2011-12 audit of information security. Our objectives included determining if the project's organizational structure and communication efforts are in compliance with UC Policy BFB IS-10, *Systems Development Standards*, and whether the project is in compliance with selected provisions of University of California (UC) Policy BFB IS-3, *Electronic Information Security*. We also assessed the progress of management corrective actions taken to address previous audit findings from the fiscal year 2011-12 audit of information security.

The results of our work disclosed no significant weaknesses in compliance with relevant UC policies. We did identify opportunities to improve the perceived accuracy of project cost reporting, and to enhance oversight and governance of the project by formalizing a steering committee charter, broadening steering committee membership, and improving communication with campus stakeholders. Our review also found that there has been significant progress on the issues identified in our previous audit of information security, although these prior recommendations have only been partially addressed due to the complexity of the relevant action plan and other project priorities.

Detailed observations and management corrective actions are included in the following sections of the report. The management corrective actions provided indicate that each audit observation was given thoughtful consideration and positive measures have been taken or planned in order to implement the management corrective actions. The cooperation and assistance provided by Student Information Systems & Technology and other personnel during the review was sincerely appreciated. If you have any questions, please feel free to contact me.

Respectfully submitted,



Robert Tarsia
Director
Audit and Advisory Services

Enclosure

cc: Chancellor Henry Yang
Vice Chancellor for Student Affairs Michael D. Young
Senior Associate Vice Chancellor Marc Fisher
UCSB Audit Committee
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca

Student Information Systems & Technology
James Kinneavy, Director, Strategic Architecture & Platform Integration Services
Diana Antova, Director, Data Services & Business Systems Support

.

PURPOSE

This audit was a limited scope progress review of the Student Information Systems (SIS) Modernization Project. The original purpose of this audit was to review the status of the refinement and other tasks scheduled for the period after Phase 1 of the project (SIS Conversion). Due to delays in initiating our audit, we revised our purpose to include a review of selected areas relevant to the project from February 2013 to February 2014, as well as follow-up of related issues from a fiscal year 2011-12 audit of information security. This audit is part of the fiscal year 2013-14 audit services plan of University of California, Santa Barbara (UCSB) Audit and Advisory Services.

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of the review was limited to activities and information related to the SIS Modernization Project, from the end of Phase 1 in February 2013, through February 2014, along with related issues from a fiscal year 2011-12 audit of information security.

Our audit objectives included the following:

- Perform a project risk assessment to gain an understanding of the current state of the project through a review of existing project documentation and interviews with Student Information Systems and Technology (SIS&T) managers and technical personnel. The purpose of this risk assessment was to identify and prioritize key project risk areas for additional analysis and audit efforts.

- Determine if the project's organizational structure and communication efforts are in compliance with University of California (UC) Policy BFB IS-10, *Systems Development Standards* (Policy IS-10) and best practices.

- Determine if the project is in compliance with selected provisions of UC Policy BFB IS-3*, Electronic Information Security* (Policy IS-3).

- Assess the progress of management corrective actions taken to address previous audit findings from a fiscal year 2011-12 audit of information security; these issues involved user access controls and review of privileged user activity.

To accomplish our objectives, our detailed work included interviews, direct observations, review of documentation, and other steps:

- Review of UC policies related to system development and security:

    - BFB-IS-2, *Inventory, Classification, and Release of University Electronic Information* (Policy IS-2)
    - BFB IS-3, *Electronic Information Security* (Policy IS-3)
    - BFB IS-10, *Systems Development Standards* (Policy IS-10)

- Review of project documentation available as of February 6, 2014, including the project plan, communication plan, project status reports, procedures, guidelines, relevant contracts, and various other plans, reports, and documents provided by SIS&T.

- Interviews with SIS&T managers and technical personnel involved with the project and participation in a project steering committee meeting.

- Review of project steering committee composition and communication efforts, and comparison with Policy IS-10 requirements and best practices.

- A detailed review in two areas selected based on our risk assessment, backup processes and security patch management practices, for compliance with Policy IS-3.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

BACKGROUND

Replacement of the legacy student registration and admissions systems was planned for a number of years. In early 2007, an SIS Strategic Planning group was formed to analyze the risks associated with the aging student systems and suggest alternatives for replacement. One of the primary drivers for the project was the need to migrate the systems due to the obsolescence and planned replacement of the campus mainframe.

In 2008, an initial decision to replace SIS with a new, externally-purchased system was abandoned after determining that it would be cost prohibitive to fully adapt/integrate the current SIS structure with the selected system platform. Management subsequently decided to convert the systems to a modern platform, utilizing external vendors and a division of technical personnel. The first phase of the project involved the conversion of 18 student information systems used by the Student Affairs Division, academic and other campus administrative offices, and current and prospective UCSB students. The overall project is currently divided into three phases:

- Phase 1 - SIS Conversion: This phase involved the migration of the existing core mainframe-based (Natural/Adabas) Student Registration and Records, Admissions, and Graduate Division systems to a Microsoft technology (.NET / SQL Server). The SIS Conversion phase started in February 2011 and was completed in February 2013. After the conversion, the new applications were accessible through a web interface.

- Phase 2 - SIS Stabilization: This phase was not in the original project plan, but was incorporated into the project at the end of Phase 1. Due to the cyclical nature of UCSB business, this period allowed the project team to use the converted applications for one year while closely monitoring system performance, and to resolve any issues that arose. In addition, additional services, infrastructure, security enhancements, and interfaces were implemented to make the system completely functional, and to improve the server environment and deployment process. The SIS Stabilization phase started in February 2013 and was completed in February 2014. Table 1 outlines the main Phase 2 milestones.

Table 1 **Timetable for Key Milestones/Tasks February 2013 to February 2014**

Milestone/Task	Initial Projected Start Date	Initial Projected End Date	Actual Start Date	Actual End Date
Admission System Stabilization	2/19/13	2/28/14	2/19/13	2/28/14
Registrar Systems Stabilization	2/19/13	11/28/14	2/19/13	2/28/14
Graduate Division Systems Stabilization	2/19/13	2/28/14	2/19/13	2/28/14
Financial Aid System Stabilization	2/19/13	2/28/14	2/19/13	2/28/14
Common Components and Services	2/19/13	2/28/14	2/19/13	2/28/14
Infrastructure and Security Improvements	2/19/13	2/28/14	2/19/13	2/28/14
Data Services	4/22/13	2/28/14	2/22/13	2/28/14
Security and External Data Integration	12/18/13	2/28/14	12/18/13	2/28/14

Source: Auditor Analysis of SIS Modernization Project Plans through February 2014.

- Phase 3 - SIS Modernization: This phase is focused on developing and implementing services, components, and application infrastructure that are critical for the success of the project. The SIS Modernization phase started in February 2014 and will be completed in February 2015, with additional project work required at least through mid-2017. Phase 3 includes the following projects:

    - Online Portal/SSO
    - Service-Oriented Application Infrastructure
    - Business Workload Automation
    - Business Process Automation
    - Deployment Automation Architecture Improvements
    - Web Application Infrastructure Improvements

Project Costs

Table 2 summarizes actual and projected costs over the life of the project. As of January 2014, the total project cost was estimated at $14.3 million.

The total estimated cost includes $6.9 million in estimated internal costs, an estimate that has remained the same since the time of our last review in fiscal year 2012-13.[1] According to SIS&T, the estimate was performed at the beginning of the project for internal resource planning purposes only. SIS&T indicated to us that it is not critical or cost-effective to fully track internal costs related to this project, due to the complexity of the student information systems; thousands of interfaces and relationships with other applications, data repositories, and processes; utilization of division-wide shared infrastructure, technical operations support, technical resources, and professional expertise; and required changes and enhancements, some of which

[1] Internal costs include payroll and benefits of internal personnel working on the project.

have been dictated by changing internal and external requirements, including mandates from UC Office of the President (UCOP).

Steering Committee

The Project Steering Committee for Phase 1 was responsible for the establishment, review, and approval of the project budget and modifications, and any significant changes in project status and use of project resources. This committee included 17 members from different campus departments, nine of whom were Student Affairs personnel. For Phase 3, the newly reformulated Modernization Steering Committee is composed of 11 members, 10 of whom are Student Affairs personnel.

Table 2 SIS Modernization Project Costs

Cost Category	FYs 2010-2013 Cumulative	FY 2013-14 (Estimated)	FY 2014-15 (Estimated)
Planning	$ 40,000	$ 30,000	$ 0
Infrastructure	414,231	170,000	170,000
Licensing	133,794	132,500	157,500
IT Service Vendors	2,672,877	25,000	0
Additional Staff/Backfills	1,590,309	642,659	632,659
Travel/Training	76,387	25,000	15,000
Supplies/Materials	83,537	10,000	10,000
Contingency (10-20%)	0	155,274	197,032
Subtotal	**$ 5,011,135**	**$ 1,190,433**	**$ 1,182,191**
Estimated SIS Modernization Project External Costs			**$ 7,383,759**
Internal Costs	$3,220,097	$ 1,927,500	$ 1,760,625
[1] **Total Internal (Admin/IT Staff) Costs**			**$6,908,222**
		[2] **Project Costs Total:**	**$14,291,981**

Source: Auditor Analysis

[1] This value is based on estimates at the beginning of the project.

[2] For purposes of comparison to project costs reported previously, additional SIS modernization costs of $832,364 for fiscal years 2008-09 and 2009-10, incurred prior to the application conversion phase, were not included in this total. Including these costs brings the project costs total to $15,124,345.

SUMMARY OPINION

The results of our work disclosed no significant weaknesses in compliance with relevant UC policies. We did identify opportunities to improve the perceived accuracy of project cost reporting, and to enhance oversight and governance of the project by formalizing a steering committee charter, broadening steering committee membership, and improving communication with campus stakeholders. Our review also found that there has been significant progress on the issues identified in our previous audit of information security, although these prior recommendations have only been partially addressed due to the complexity of the relevant action plan and other project priorities.

Audit observations and management corrective actions are detailed in the remainder of the audit report.

DETAILED OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. Validate Internal Cost Estimate

As described in the Background section of this report, the estimated total cost of this project includes $6.9 million in internal costs, an estimate that has remained the same for several years. According to SIS&T, the estimate was performed at the beginning of the project for internal resource planning purposes only. SIS&T indicated to us that it is not critical or cost-effective to fully track internal costs on an ongoing basis, because costs were carefully and fully defined before the implementation phase. Policy IS-10 requires estimates for the time needed for administrative computing department staff on a project, and sound project management practices require ongoing monitoring of time and project costs. For these reasons, and because the estimated internal costs are substantial, representing 48% of the total estimated project cost of $14.3 million, it would be prudent to validate the existing estimate.

We understand that a current estimate of internal costs may actually be lower than the existing figure. Regardless, the perceived accuracy of project cost reporting would be enhanced by including a recently validated, updated estimate for internal costs.

Management Corrective Actions

To ensure that our project cost reporting is seen as completely accurate; Student Affairs will review our estimate for internal costs and update our reporting, if needed.

Audit and Advisory Services will follow up on the status of this issue by September 30, 2014.

B. Enhancing SIS Modernization Project Oversight and Governance

1. A Steering Committee with Broader Representation

Our audit identified opportunities to enhance oversight and governance of the project.

Formalizing a Charter

It is our understanding that a steering committee charter has not been formally documented. Without a formally documented charter, the project's steering committee may be limited in its ability to provide appropriate guidance, direction, and oversight. Going forward, a formalized charter would define the purpose, objectives, and roles of the Project Steering Committee and its members, and would detail the required commitment and decision-making responsibilities of committee members.

Steering Committee Size and Composition

For large projects, Policy IS-10 recommends having a high-level steering committee composed of senior-level management for functional offices, the "administrative computing department", and internal audit, if appropriate.

As discussed in the Background section, the Project Steering Committee for Phase 1 and Phase 2 was composed of 17 members from different campus departments. Although nine of the committee members were Student Affairs personnel, the committee included fairly broad representation of central IT departments and other stakeholders. For Phase 2 and Phase 3, the newly formulated Modernization Steering Committee is composed of 11 members, 10 of whom are Student Affairs personnel. Central IT departments are not represented, and only one member is from another stakeholder group.

Table 3 **Steering Committee Membership**

	Phase 1 & 2	Phase 3
Student Affairs	9	10
Central IT Departments	3	0
Other Stakeholders	5	1
TOTAL	**17**	**11**

Source: Auditor Analysis

To help ensure adequate visibility and support for this critical campus project, Student Affairs should consider broader representation, including members from central IT departments and other stakeholder units.

Management Corrective Actions

The steering committee had broad campus involvement for Phase I, and participation naturally contracted when the project entered Phase II (bug fix and stabilization). Phase III is primarily about creating infrastructure and architecture that will support future growth of student information systems. As such, Phase III mostly does not include student or faculty-facing capabilities and, therefore, the interest group for this is very narrow. Where appropriate, we are including broader representation. For example, the effort to improve iSIS screens will include a focus group with campus-level representation.

Audit and Advisory Services will follow up on the status of this issue by September 30, 2014.

2. Improving Transparency and Communication

We found that SIS&T has implemented project communication processes that are effective overall. We also found, however, that communication processes have recently been focused largely on operational activities and internal communication for project team members, and have not included enough timely information for the campus community. For example, the project status cannot currently be determined from SIS&T's website, which was not updated from December 2012 to January 2014.

At the time of our review, the website content included:

- The *SIS&T Portfolio Projects and SIS&T Accomplishments Report* from fiscal year 2011-12.
- An organizational chart that does not include the names of SIS&T personnel, and dated steering committee membership information from Phase 1 of the project.

The SIS Modernization Project is a strategic project for the UCSB. As Phase 3 progresses, there are opportunities to improve the effectiveness of communications to ensure that the campus community is informed of project goals and achievements.

We recommend that SIS&T improve campus-wide communication through:

- More frequent communications to the campus, possibly as part of a more robust communication plan.
- An updated website that includes current project reporting, organizational information, and steering committee membership.

Management Corrective Actions

For Phase III, SIS&T will update the project website quarterly with information on project status, milestones, and issues. We will communicate accordingly when there are any developments or issues that could have a broad campus impact; however, because of the narrow technical focus of the project at this point, there is no need for a formal campus communication plan.

Audit and Advisory Services will follow up on the status of this issue by September 30, 2014.

C. UC Policy IS-3 Compliance Requirements and Best Practices

Our review found full compliance with Policy IS-3 requirements for backup processes and patch management practices. The overall purpose of our work was to confirm that project activities incorporate the proper maintenance and data recovery measures and patch management practices, as required by Policy IS-3. Table 4 summarizes our findings.

1. Backup Process

   Policy IS-3 requires that system administration practices include routine backup of applications and data. To evaluate compliance with this requirement, we determined whether:

   - A backup policy has been documented and includes retention period requirements.
   - Backup copies of essential data for disaster recovery purposes are stored at an off-campus site.
   - Backups are encrypted before they are sent off campus.
   - Recovery tests have been regularly performed.
   - There are sufficient resources for emergency planning and disaster recovery.
   - Other related requirements are met.

We found that the project's backup processes meet relevant requirements, and should ensure that there are adequate protections for data and its confidentiality.

2. Patch Management Practices

Policy IS-3 requires that systems personnel timely update versions of the operating system and application software for which security patches are made available, in conformance with change management processes and campus minimum standards.

We evaluated whether:

- The firewall operating system is the newest version, or the installed version does not have any critical vulnerabilities.
- Patch management procedures have been documented.
- Patch management practices can identify if announced security patches have been installed.
- Scans of vulnerabilities are performed regularly.

Table 4 UC Policy IS-3 Compliance

Area	Tested	
Backup Process	✓	Backup Policy
	✓	Backup Stored at Off-campus Site
	✓	Backups Encrypted
	✓	Data Recovery Tests
Patch Management Practices	✓	Patch Management Procedure
	✓	Security Patches in Servers
	✓	Firewall Without Vulnerabilities
	✓	Scan of Vulnerabilities

Source: Auditor Analysis

We found that SIS&T uses *Windows Software Update Server* (WSUS) to manage Student Affairs server updates, and that the process is documented in a brief procedure. No significant issues were observed in the status of server updates. We also found that the firewall did not yet have the last operating system version installed; however, no critical vulnerabilities have been identified related to the current operating system, and SIS&T plans to update the operating system when appropriate. We also found that patch management processes are reasonable, and can identify and update critical security patches in a timely manner.

D. Status of Issues Addressed in Previous Audits

Our 2011-12 *IS-3 Electronic Information Security* audit included two recommendations related to user access reviews across registration systems and activity logs of system administrators.

Based on the result of our review, we found that action plans are in place and there has been significant progress on the issues addressed. However, both recommendations are only partially addressed due to the complexity of the action plan and other project priorities. Table 5 summarizes the status of the issues.

Table 5 Status of Management Corrective Actions

Finding Title	Status	Activities in Progress
User Access Reviews Not Performed	**Partially Implemented**	Automation of Audit Logs, Reporting and Workflow Review
		Developing a Cross-Reference Between Campus Identity Manager and SIS Active Directory
		Implementation of Audit Tool
Lack of Administrative/ Privileged User Activity Log Reviews	**Partially Implemented**	Centralizing Network and Server Access Logs

Source: Auditor Analysis

1. User Access Reviews Not Performed

   Our 2011-12 audit found that supervisors or other employees with responsibilities for security did not periodically review the system administration work of personnel with access to privileged accounts, as required by Policy IS-3.

   Since that time, SIS&T has taken steps to address this issue, including:

   - Collecting and verifying user privileges on database servers.
   - Updating inactive and disabled SIS Active Directory accounts.[2]
   - Reviewing key administrative functions and adjusting user groups.
   - Developing a basic framework for common roles and privileges.
   - Evaluating products for auditing and reporting privileges for the SIS&T Active Directory, SIS server file systems, and SIS databases.
   - Starting the automation of change identification in employee status or department assignment.
   - Selection of an auditing tool.

[2] The SIS Active Directory is a central repository that contains user IDs and user permissions for identity management for SIS applications.

The following additional activities in the action plan are in progress:

- Automating auditing, reporting, and workflow.
- Developing an interface between the campus identity management system and the SIS Active Directory.

2. Lack of Administrative / Privileged User Activity Log Reviews

Our 2011-12 audit found that logs of administrative/privileged user activity were not being performed. These reviews are necessary to ensure that only authorized individuals are granted access, and that activity is appropriate. As required by Policy IS-3, user access reviews should be performed on a regular basis through the review of access lists that are generated by the relevant IT organization.

It is our understanding that the project team is addressing these issues at this time. Since the time of our audit, SIS&T has evaluated several products to assist in this process, and has temporarily installed an evaluation version of one of them to better understand the capabilities and management impact. SIS&T is also currently considering an auditing tool to centralize the review of SIS network and SIS server access logs.

Management Corrective Actions

1. User Access Reviews Not Performed

Since the last follow-up on this issue by Audit and Advisory Services, SIS&T has continued to make progress on this issue. We have:

- Selected an Active Directory auditing tool, which will be implemented during the summer of 2014.
- Performed an extensive review and cleanup of Active Directory accounts, including privileged access, during the 2013-14 year.

An automated report of employee separations and other departmental changes is under development, and will be completed by the end of the summer of 2014. An automated workflow for employee de-provisioning is planned, but is on hold due to other project priorities. It is currently in our project backlog awaiting prioritization.

2. Lack of Administrative / Privileged User Activity Log Reviews

The SIS&T team met on several occasions in the late 2013, early 2014 to discuss approaches. Action on this was deferred pending a selection of an Active Directory auditing tool to determine what level of functionality might be available via the selected tool. It was determined that the selected tool does not currently meet this need. Log centralization is the first step to enable this type of auditing and is currently in the project backlog queue awaiting prioritization.

Audit and Advisory Services will follow up on the status of this issue by January 31, 2015.