



Secretary of State Audit Report

Oregon University System Application Controls Review of Oregon State University Banner Student Information System

Summary

PURPOSE

The purpose of the audit was to evaluate whether selected data processed by Oregon State University's Banner Student Information System remained complete, accurate, and valid throughout the data management process, and to evaluate the processes used for change management, physical and logical security, and disaster recovery and contingency planning.

RESULTS IN BRIEF

We determined that Oregon State University's Banner Student Information System generally maintained the completeness, accuracy and validity of the data; however, we found several minor data input and processing weaknesses warranting management's attention. We also found that processes relating to security, disaster recovery and business continuation planning, and system maintenance could be improved.

We identified other issues during our audit that we believed deserved the attention of the university, but did not warrant reporting in the audit report. These issues were conveyed in Management Letter No. 580-2004-04-01, dated April 2004.

We communicated to six of seven universities and the Chancellor's Office our assessment of risks based on each entity's response to survey questions. These communications are in Management Letter Numbers 580-2003-09-01 through 580-2003-09-07, dated September 2003. Because of the sensitive nature of the risks relating to security, these were communicated in confidential attachments where appropriate. This confidential information was prepared in accordance with ORS 192.501 (23), which allows exemption of such information from public disclosure.

RECOMMENDATIONS

We recommend that management:

- Improve data input controls to correct weaknesses in reporting student resources and retaining grade documentation.

- Correct processing errors identified during the audit.
- Improve data processing controls to better detect and correct errors and separate key responsibilities.
- Enforce procedures for managing and resolving financial aid over awards.
- Collect overpayments and under assessed tuition and fees as appropriate.
- Develop and implement an overall security policy.
- Formally assign the responsibility for the security of its information assets to an information security manager.
- Improve controls over logical access to better manage security activities.
- Improve physical access controls to better protect computer systems and electronic information.
- Fully develop its business continuation plans, fully test the plans, provide training to appropriate staff, and develop suitable distribution lists. Place a copy of the business continuation plans offsite.
- Regularly verify the usability of backup files.
- Move its offsite storage facilities to appropriate locations.
- Consider relocating its network and telecommunications facility to an appropriate location.
- Develop and implement formal change management procedures and establish an appropriate environment for development activities.

AGENCY'S RESPONSE

Oregon State University of the Oregon University System generally agrees with the recommendations.

Background

Oregon State University (university) relies on its Banner Student Information System (system) for recording and managing student and academic data, including financial aid information and student financial accounts. This information is contained in three system components administered by university business units.

The component administered by the Registrar's Office stores the official academic records for students, the course catalog, class schedule, and instructor information.

The Office of Financial Aid and Scholarships administers the component that processes financial aid applications. Students routinely interact with the Office of Financial Aid and Scholarships through the Web to complete require-

ments and accept, decrease, and reject awards.

The accounts receivable component, administered by the Office of Business Affairs, maintains student financial account information. This component receives electronic information from other departments, such as University Housing and Dining Services and the Office of Financial Aid and Scholarships. This component records tuition and fees, other charges, and payments to student accounts. It produces information for billing students and preparing refunds.

According to university information, the Registrar's Office served approximately 21,700 students during the period Summer Term 2002 through Spring Term 2003. Tuition and fees assessed were approximately \$102 million and

financial aid paid was approximately \$90 million.

Information System Controls

Information system controls are typically classified as general controls or application controls. General controls protect the environment in which software applications process data. Application controls relate to specific processing requirements of individual software applications. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Application controls coupled with general controls provide more assurance that transactions processed through the system are authorized, reliable, and complete.

Audit Results

We determined that the system generally maintained the integrity of the data; however, we identified application controls relating to data input and data processing and various general controls that could be improved.

Application Controls

Application controls include methods for ensuring that only complete, accurate and valid data are entered in a computer system; processing performs the correct functions and results are accurate; and data are properly maintained. These controls may be either manual or automated.

We reviewed the university's application controls over the Banner Student Information System (system) related to academic records, financial aid, and student accounts receivable.

Data Input

Controls over data input ensure that input errors are detected, reported, and corrected prior to processing and as close to origination of the error as possible. Procedures should also be in place to ensure original source documents are retained or are reproducible by the organization for an adequate amount of time to facilitate retrieval or reconstruction of data.

Reporting of Student Resources Needs to Be Improved

The system did not have complete information for the process of assessing financial aid needs for a small population of students. Students can receive financial support from various sources apart from the financial aid office. This support is considered a resource to the student and could reduce their financial aid.

The university did not consider one type of support in the financial aid award process for 92 students because it did not have adequate controls to help ensure that all resources were reported to the financial aid office. We reviewed awards for four of these students and found one student may have received approximately \$1,200 more in grants than what she should have received.

Grade Documentation Not Always Retained

Student grades listed in the system were not always supported by source documents. According to the university's archives schedule, these records should be retained for two years by university departments.

The departments did not retain adequate documentation for 12 of 50 grades tested. We verified the accuracy of these grades using other procedures.

Audit Results

Grades affect students' academic standing which, in turn, can affect their eligibility for financial aid. Questions about a student's academic standing could best be resolved if source documentation for grades is available from departments.

We recommend that management improve controls to help ensure that all student resources are reported to the financial aid office.

Agency's Response:

We agree with this recommendation. Business Affairs has developed a standard process for reporting to Financial Aid. On a bi-weekly basis, a hard copy spreadsheet for third party support payments and/or scholarships, processed through Business Affairs, is forwarded to Financial Aid showing all activity during that bi-weekly period, to include student name, ID, amount of payment, and funding sponsor. Implemented December 2003.

We also recommend that management retain grade documentation as required.

Agency's Response:

We agree with this recommendation. Periodically, the Registrar's Office will notify academic departments of the need to retain grade documents according to the University's retention schedule. First reminder will occur by May 1, 2004. Subsequent reminders will be given during Fall and Spring Terms of each academic year.

Data Processing

Controls over data processing ensure that all data that has been input is correctly processed and conforms to predetermined criteria. The department relies on various automated routines to meet its processing objectives. For example, tuition and fee charges are assessed based on the registration information entered for a student.

We tested some of the key processing routines and noted that the system did not always correctly assess tuition and fees.

Tuition Not Always Assessed

Under limited circumstances, system processing did not assess tuition to students who should have been charged. We identified three students who took a total of 19 credit hours but were not charged tuition. As a result, the university did not collect approximately \$1,500 in tuition. In addition, the university did not have a process to find and correct these errors.

Tuition and Fees Not Always Correct

Under limited circumstances, system processing incorrectly assessed tuition and fees on student accounts. The university identified this issue before our audit, but had not determined the cause or the number of students affected. A manual process was in place to identify and correct these errors; however, the process did not identify all occurrences and did not ensure all errors were corrected when found.

For example, we found three instances of incorrectly assessed tuition and fees, one of which had previously been identified by the university's process, but had yet to be fully corrected 10 months later. The errors on each of the three accounts did not exceed \$100. They represented both over and under charges. Because the total number of accounts with assessment errors was unknown at the time of our review, we were unable to determine the overall dollar effect.

We recommend that management correct processing errors and improve the manual controls over identifying and investigating tuition and fee errors.

Agency's Response:

We agree with this recommendation. Business Affairs is currently designing the recommended audit process, and upon completion will forward the work order to Central Computing for implementation. Business Affairs will be re-

viewing accounts to determine where adjustments could be made and where, due to the purge of registration records on the standard purge schedule, they are unable to determine an accurate adjustment.

Tuition Not Always Assessed: In conjunction with the auditors, we have identified approximately \$24k in un-assessed tuition, which represents approximately .0003% of the overall tuition revenue in the 2003 fiscal year. On a go-forward basis, we have developed an audit report that identifies students that have registered and have no tuition assessed. We are running this audit report each term after the 4th week.

Tuition and Fees Not Always Correct: In conjunction with the auditors, we have identified approximately \$15k in incorrect tuition assessments that represents approximately .00019% of tuition revenue in the 2003 fiscal year. On a go-forward basis, we have expanded our refunding rules to account for all dates within a term, creating a 0% refunding rule for activity after the 4th week. As an additional control, we are reviewing each tuition assessment that occurs after the 4th week for appropriateness or adjustment. We will perform this review for each term.

Scheduled implementation is Winter Term 2004.

Over Award Procedures Need to Be Enforced

Procedures to manage and resolve financial aid over awards were not always followed. A student is considered over awarded if their award amount is greater than their financial need. This condition can occur if additional resources are reported for the student after their initial financial aid has been awarded. Staff is to review the award for these students and make adjustments to reduce undistributed amounts as necessary.

Audit Results (continued)

We reviewed 10 students who were in an over awarded condition. Three of these students received payments after their additional resources were reported. As a result, the university overpaid these students approximately \$3,800.

We recommend that management enforce procedures for managing and resolving over awards.

Agency's Response:

We agree with this recommendation. The Financial Aid Office will work with the programming staff to design a Banner report to identify over-awards. The report will be scheduled regularly on a monthly basis through the Production Schedule. Scheduled implementation is October 2004.

Responsibilities Not Separated

Staff with responsibilities for setting up fee assessment codes in the system performed and reviewed their own work. As a result, errors could be recorded and not be detected or corrected. For example, at least two students had an \$87 fee reversed on their account although they were never charged the fee. This was the result of a fee assessment coding error. Errors on these accounts occurred in Summer Term 2002 and had not yet been corrected when we reviewed the accounts in September 2003.

Management is responsible for assigning responsibilities to ensure that no one individual controls all key aspects of a transaction or event. Further, the work performed should be routinely reviewed by an independent person.

We recommend that management separate responsibilities for the fee assessment process to allow for review of the work performed.

Agency's Response:

We agree with the recommendation. Duties will be separated as follows: one person responsible for the develop-

ment and data entry of fee rules in Banner, and two others responsible for reviewing rules and testing fee assessment. A test suite of student registration profiles has been established. The new review process will be established by September 2004.

Finally, we recommend that management collect the overpayments and under assessed tuition and fees identified in the above sections, as appropriate.

Agency's Response:

We agree with the recommendation. Based on data collected by OSU personnel during the process of this audit, adjustments to assessments and billings will be made. Implementation will be by May 2004.

General Controls

General controls protect the environment in which software applications process data. These controls relate to physical and logical security, backup and recovery of data, business continuation planning, change management, and other organizational responsibilities.

Information Security Management

Management is responsible for establishing controls to protect information assets through effective information security management. Two key elements of an information security management process are policies and procedures and organization.

Management's security policies and procedures should start with a high-level policy specifying, among other items, management's direction for security, its purpose and objectives, the management structure, and the scope within the organization.

Organization encompasses the definition and assignment of responsibilities for implementation of security processes at all levels.

The university had security policies and procedures that communicated management's expectations for students' and employees' use of information assets and the protection of confidential data from public disclosure. The university had not, however, established policies and procedures that communicated the following:

- Management's overall purpose and objectives for the security of information assets.
- The management structure as it relates to security.
- The scope within the organization.
- The definition and assignment of responsibilities for implementation at all levels.

Although the university had assigned the responsibilities for protecting individual assets to various staff, it had not formally assigned responsibility for security to an information security manager.

As a result, the university's controls for safeguarding information assets may not be administered in line with management's intentions. Specifically, logical access controls and physical access controls may not be consistently implemented, and expected elements may be missing as discussed in the next two sections of this report. Furthermore, management is less able to ensure that its information assets are adequately protected from unauthorized use, destruction, modification, and disclosure.

We recommend that management develop and implement an overall policy providing direction for its security management.

Agency's Response:

We agree with the recommendation. OSU will form a Security Committee that will meet regularly (semi-annual meetings, plus emergency meetings) to plan policies and amend policies as

Audit Results (continued)

new issues surface. The Committee will consist of appropriate administrative representatives from Information Services and Finance and Administration. A Security Committee will be operational by September 1, 2004, with an initial policy completed by February 2005.

We also recommend that management formally assign the responsibility for assuring security of its information assets to an information security manager.

Agency's Response:

We disagree with this recommendation. We concur that centralized management of security of information assets is necessary. However, we believe that a security committee provides a more effective methodology for developing a security policy with appropriate advice and guidance from all of those with an investment. A Security Committee will be operational by September 1, 2004, and they will assume this responsibility by December 31, 2004.

Logical Access Controls

Logical access controls are the primary means of safeguarding information against unauthorized use, disclosure or modification, damage or loss by restricting access to authorized users on a least-need basis.

The university relies on various manual and automated controls to limit access to the system. For example, the university requires requests for access to be approved by designated managers. In addition, the system forces periodic password changes and a minimum password length.

We tested the university's logical access controls and found areas where policies or procedures were needed to strengthen controls. We also found that improvements could be made in administering security procedures.

Policies and Procedures Needed

The following areas lacked policies or procedures:

- The university had not established a policy to revoke employees' access within a minimum time period after termination of employment. As a result, not all user accounts were deactivated in a timely manner. Access for 147 of 276 employees continued an average of 72 days after their termination dates. Three additional employees continued to have active system access at the time of our review even though they had terminated employment 24 to 55 days prior to our test. In addition, 12 employees accessed the system after their termination dates. The university could not determine the extent of the access used.
- Procedures had not been developed for obtaining management's authorization for granting employees a secondary level of security access.
- Written criteria for granting access were not fully developed.

We recommend that management develop and implement policies and procedures to deactivate user accounts no later than the end of the employee's last workday.

Agency's Response:

We agree with this recommendation. Knowledge of an employee's last work date is resident at the departmental level. Departments currently report the employee termination dates to Human Resources, who then enter the dates into Banner. However, the employee's last workday may precede their termination date.

The University will convene a working group, which will include representation from Human Resources and Information Services, to develop a streamlined process providing notification of the appropriate offices to ensure

timely revocation of system access. The scheduled implementation date is December 31, 2004.

We also recommend that management:

- Require authorization for the secondary level of access security.
- Ensure that written criteria for granting that access is fully developed.

Agency's Response:

We agree with these recommendations. Written criteria for granting access is being written by Central Computing, for approval of the granting departments. The completion date for this action is August 31, 2004.

Security Administration Needs Improvement

Procedures were not adequate or were not administered properly in the following circumstances:

- Programmers had unlimited access to the production programs and data.
- Shared user IDs were used in certain circumstances.
- At least 16 employees had the ability to register students for courses and control a portion of the billing process for those courses.
- Too many employees had access to modify one key security function. Management indicated this access would be removed for five of nine employees.
- Password parameters were not always set at optimum levels.
- Not all student users were required to sign security agreements, contrary to university policy that required all users to sign these agreements. Furthermore, users were not required to periodically update their security agreements.

Audit Results (continued)

We recommend that management restrict programmers' access to production to only emergency situations and closely monitor these activities.

Agency's Response:

We agree with this recommendation. To balance the situation of unlimited access to the production database and the need to be certain that programmers have sufficient access to respond to emergencies as any time of day or night, as well as weekends, we are implementing the following change.

We will remove insert, update and delete permissions from each programmer's Oracle User ID. A different Oracle User ID will be created for each programmer that does have insert, update, and delete privileges. The Oracle audit trail for logins will be monitored for the use of special user IDs. Procedure will be for Central Computing management to be notified if it is necessary to make updates to the production database. If a manager cannot be reached in an emergency the programmer could make updates and would produce written verification of modifications made. Unauthorized use of the special user IDs would be cause for disciplinary action. New Oracle logins and audit trail processes will be completed by September 30, 2004.

We recommend that management eliminate shared user IDs.

Agency's Response:

We agree with this recommendation, with one exception noted below. All shared IDs in the Financial Aid Office were eliminated in February 2004, and those in the Registrar's Office were eliminated in March 2004.

Exception: Shared user IDs are still used at the customer service counter of Business Affairs where shared computers are used by a group of office personnel. The access on the shared ID is limited to query only, and is more restrictive than each individual's per-

sonal access. No changes or modifications can be made to records at the shared terminals. Additionally, the machines are physically located in a secure location and are only available to authorized staff. Access to these machines will be reviewed on a regular basis and passwords will be changed when any individual with login capability is transferred/terminated from the office. Implementation completed on March 31, 2004.

We recommend that management remove employees' conflicting and excess access.

Agency's Response:

We agree with this recommendation. The access to the "key security function" has been limited as agreed, by the reduction of the number of employees that had access to the "one key security function". In addition, we will explore functionality within Banner, and the possibility of a change in business workflow, for a solution to conflicting access. Also, an exception report is now in place that provides an audit for un-assessed tuition, which will also ensure that this access is not used to register a student for courses without billing them. We will review the number of personnel with registration access. Registration access review will be completed by May 2004, and options for change in Banner access, or business workflow, will be developed by October 2004.

We recommend that management improve password parameter settings.

Agency's Response:

We agree with this recommendation. To mitigate the problem noted, the password parameter settings have been improved. Implementation of change is March 31, 2004.

Finally, we recommend that management enforce the policy to require all users to sign security agreements and require users to periodically update their security agreements.

Agency's Response:

We agree with this recommendation. When students are employed in the Registrar's Office, all student employees will sign security agreements.

Physical Access Controls

The university is responsible for restricting physical access to its information assets in order to protect its computer systems and electronic information.

The university used a combination of metal keys and electronic locking devices to secure its system hardware and network equipment. Designated managers and delegates grant authorization for metal keys and access codes. The Oregon State University Facilities Services Key Shop (Key Shop) is responsible for issuing metal keys and maintaining an inventory.

We reviewed the university's physical access controls and found the following areas needing improvement:

- Fifteen metal keys had been lost or had not been returned when access was no longer needed. Management had not changed locks at its information system facilities since the keys were known to be missing.
- There is no physical barrier separating system hardware from a publicly-accessible area within one of the university's information system facilities. The university relies on staff to prevent unauthorized access to system hardware.
- Staff who otherwise would not need access had access to network equipment because a copier, water cooler, and refrigerator were located in the same room that houses the network equipment.
- Authorizations for electronic access codes were not required to be in written format. Authorizations that were documented were not retained.

Audit Results (continued)

- Key Shop inventory records did not completely agree with the information services department records. For example, department records showed eight individuals with keys that were not listed on the Key Shop's records. According to university records, these were current employees who needed access.

We recommend that management improve physical access controls over its information assets by changing locks on a periodic basis or consider implementing a system to provide access to authorized persons only during appropriate times for their job duties, to provide an audit trail for access, and to provide a mechanism for immediate revocation.

Agency's Response:

We agree with this recommendation. An electronic key system has been installed. This system provides a mechanism for immediate revocation and an audit trail. Implementation completed March 31, 2004.

We recommend that management consider erecting a wall in the facility described above to better secure system hardware.

Agency's Response:

We agree with this recommendation. A wall has been erected that divides the Production Control area from the Machine room area. Implementation completed March 31, 2004.

We recommend that management restrict access only to individuals who have a direct responsibility for operating or monitoring network equipment.

Agency's Response:

We agree with this recommendation. Only individuals with a direct responsibility for the Computer Center machine room equipment and their managers will be given electronic keys to this restricted area. In the Network Engineering machine room the water cooler has been relocated, with refrig-

erator and copier to be moved in early summer. Implementation completed June 30, 2004.

Finally, we recommend that management improve controls over the locking systems by requiring and retaining written documentation of electronic code access authorizations and coordinating with Key Shop personnel to correct inventory records of metal keys.

Agency's Response:

We agree with this recommendation. Written authorization for access is required and retained [January 13, 2004]; and in coordination with the OSU Key Shop, electronic locks were purchased and installed, and their records should now be correct. Implementation completed March 31, 2004.

Ensuring Continuous Service

Disaster recovery and business continuation planning is necessary to ensure that services can be restored in the event of a disruption. These plans should provide detailed instructions for recovery from various disaster scenarios and be updated and tested on a regular basis. Plans should also include procedures to regularly backup information system data and store it in a secure offsite location.

The university has developed business continuation plans for its computing and network services. However, the university's overall business continuation plan has not been fully developed and implemented. Furthermore, elements of the university's information systems continuation plans were incomplete or missing, including the following:

- Disaster response scenarios from minor to total loss of capability and responses to each in sufficient detail for step-by-step execution, including users' alternative manual processing.

- Detailed lists of items necessary to recover operations. For example, the continuation plans did not specify critical data files, required recovery times, equipment and supplies, and documentation such as operating system and user manuals.
- Roles and responsibilities of key personnel needed to perform recovery and continue operations.
- Detailed procedures for recovery at an alternative site.

In addition, the university has not fully tested all of its continuation plans. It also has not provided complete training to staff, nor developed a distribution list that provides key parties with necessary information.

Furthermore, the university has not regularly verified the usability of backup files or stored copies of all business continuation plans offsite. The university's offsite storage facilities are located close enough to be subject to the same disaster as the originating site. In addition, the business continuation plan allows storage at inappropriate locations. Finally, the university's facility that houses its network and telecommunication equipment is at a location subject to flooding.

In the event of a disaster, the university may be unable to fully recover critical business operations in a timely manner.

We recommend that management fully develop its business continuation plans to include the missing elements noted above.

Agency's Response:

We agree with this recommendation. The University, via an Emergency Preparedness Steering Committee, is developing campus-wide plans to deal with emergencies or disasters. The plans will have two major components – (1) dealing with the immediacy of the disaster or emergency, and (2) business recovery/business continu-

Audit Results (continued)

ity planning. Plans will identify initial data files, required recovery times, equipment and supplies, and documentation such as operating systems and user manuals. Plans related to Central Computing will be completed by March 2005. Campus-wide plans will be completed by July 2005.

We recommend that management fully test its continuation plans, provide training to appropriate staff, and develop suitable distribution lists.

Agency's Response:

We agree with this recommendation. We will implement annual "desktop" testing and personnel training of the disaster recovery plan, with distribution as appropriate of plans and related materials. Implementation will be completed by July 2005.

We recommend that management regularly verify the usability of backup files.

Agency's Response:

We agree with this recommendation. We will verify the usability of backup files on a regular basis. Implementation will be completed by July 2005.

We recommend that management place a copy of the continuation plans offsite.

Agency's Response:

We agree with this recommendation. An off-site facility will be located, and copies of the continuation plans and other related material would be resident there. Implementation will be completed by July 2005.

We recommend that management move the offsite storage facilities to appropriate locations.

Agency's Response:

We agree with this recommendation. In addition to our campus backup storage site, we will create new a super disaster site further away from OSU where

backups will also be maintained. Implementation will be completed by July 2005.

Finally, we recommend that management consider relocating its network and telecommunications facility.

Agency's Response:

We agree with this recommendation. The relocation of Telecommunications and Network Engineering to a facility that is essentially disaster proof is an ideal concept, but one that it is unlikely the University can plan or implement in the near future due to budget constraints and competing needs. Implementation is indefinite.

Change Management

Change management is the process by which changes are authorized, planned, scheduled, applied, tested, approved, deployed, and tracked. Change management activities can impact a technology unit's ability to provide critical data processing and information delivery services. It is necessary, therefore, that each change be controlled throughout its life cycle and integrated into the production environment in a systematic and controlled manner. Situations requiring emergency changes should be defined and procedures established to ensure that all controls are retroactively applied, as normal processes are often circumvented. The methodologies should minimize the risk of disruption, unauthorized alterations and errors to systems and applications.

University management has not fully developed policies and procedures for managing changes to the system. Specifically, management has not established formal processes for:

- Approving change requests.
- Determining possible impacts on the application and operational system.
- Testing.

- Management review and approval before changes are placed into production.
- An independent migration of changes into production.
- All emergency changes.

In addition, the university has not established an appropriate environment for development activities.

As a result, management has less assurance that consistent and reliable products are delivered and that only authorized code is migrated into production.

We recommend that management make it a priority to develop and implement formal change management procedures. These procedures should include, at a minimum, the key elements listed above.

We also recommend that management establish an appropriate environment for development activities.

Agency's Response:

We agree with these recommendations. We will document the policies and procedures for approving change requests, determining possible impacts on the application and operational system, testing, management review and approval before changes are placed into production, and all emergency changes. We will install the OpenVMS DECset, which includes a code management system. We will improve the timeliness and variability of the data in the Development Database. All changes will be implemented by April 30, 2005.

Objectives, Scope and Methodology

The purpose of our audit was to evaluate the adequacy of application and certain general controls over the university's Banner Student Information System (system), specifically components for recording and managing academic history, financial aid, and student accounts receivable. The audit had the following objectives:

- Determine whether the university ensures that selected critical data for the system remains complete, accurate, and valid during its input, processing, output, and storage;
- Determine whether the university safeguards the Banner system information against unauthorized use, disclosure or modification, damage or loss;
- Determine whether the university has implemented policies and procedures and an organizational structure so that one individual cannot control key aspects of information technology operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records;
- Determine whether the university has implemented formal change management policies and procedures to prevent unauthorized modifications to the system from being implemented;
- Determine whether the university has implemented a complete and tested disaster recovery plan for the system to ensure a minimum business impact in the event of a disaster.

Prior to our audit, in February 2003 we initiated a survey of the seven Oregon universities and the Chancellor's Office about their procedures for ensuring the integrity of electronic data, security of information assets and continuous service of information resources. We analyzed the responses and assessed the risk to information assets at each entity. From this risk assessment, we selected Oregon State University for an application controls review.

We conducted our audit from February 2003 through January 2004. We limited our audit work to records relating to the period Summer Term 2002 through Spring Term 2003 except for our review of access revocation. For this work, we reviewed records of system users between 1999 and 2003.

During our audit we interviewed various university personnel, examined documents supporting controls, and analyzed electronic data. We also evaluated compliance with applicable laws, rules, and regulations pertaining to the system.

We used the Information Systems Audit and Control Foundation's (ISACF) publication, "Control Objectives for Information and Related Technology," (COBIT) to identify generally accepted and applicable internal control objectives and practices for information systems. ISACF is a worldwide organization dedicated to research, develop, and publicize control objectives and audit guidelines.

We conducted our audit according to generally accepted government auditing standards and Information Systems Audit and Control Association standards for information systems auditing.



Secretary of State
Audits Division

BILL BRADBURY, SECRETARY OF STATE
CATHY POLLINO, STATE AUDITOR, AUDITS DIVISION

255 Capitol St. NE Suite 500
Salem, OR 97310

*Auditing to Protect the
Public Interest and Improve
Oregon Government.*

AUDIT ADMINISTRATOR: *Nancy L. Young, CPA, CISA*

AUDIT STAFF: *Dale Bond, CPA, CISA, CFE*
Erika A. Ungern, CISA
Darrin D. Hotrum, CISA
Jessica E. Wicklund

DEPUTY DIRECTOR: *Charles A. Hibner, CPA*

*The courtesies and cooperation extended by the officials and staff of the
Oregon University System were commendable and much appreciated.*

*This report, which is a public record, is intended to promote the best possible
management of public resources. Copies may be obtained by mail at:*

*Oregon Audits Division
255 Capitol Street NE, Suite 500
Salem, OR 97310*

*by phone at 503-986-2255 and 800-336-8218 (hotline), or internet at
Audits.Hotline@state.or.us and
<http://www.sos.state.or.us/audits/audithp.htm>*