The University of Nebraska

Management Letter

For the Year Ended June 30, 2012

Issued on February 12, 2013

NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@nebraska.gov
P.O. Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.state.ne.us

December 14, 2012

The Board of Regents
University of Nebraska

We have audited the financial statements of the University of Nebraska (the University) (a component unit of the State of Nebraska) for the year ended June 30, 2012, and have issued our report thereon dated December 14, 2012.

Our audit procedures were designed primarily to enable us to form an opinion on the Basic Financial Statements and therefore, may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the University's organization gained during our work, and we make the following comments and recommendations that we hope will be useful to you.

INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH *GOVERNMENT AUDITING STANDARDS*

Internal Control Over Financial Reporting

Management of the University is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies, or

material weaknesses. We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified a certain deficiency in internal control over financial reporting as described in the accompanying schedule of findings and responses that we consider to be a significant deficiency in internal control over financial reporting as noted in Comment Number 1 (SAP Payables Access). A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

We also noted certain other matters that we reported to management of the University, noted in sections B and C of the following Schedule of Findings and Responses.

The University's responses to the findings identified in our audit are described in the accompanying schedule of findings and responses. We did not audit the University's responses and, accordingly, we express no opinion on the responses.

SCHEDULE OF FINDINGS AND RESPONSES

A. SIGNIFICANT DEFICIENCIES

1. SAP Payables Access

A good internal control plan includes a proper segregation of duties to ensure no one individual can process transactions from beginning to end to reduce the risk of fraud, waste, or abuse of University funds.

In Systems Applications and Products (SAP), the University's accounting system, the role "MM_AP_MAINTAIN" allows employees to enter, modify, post, and approve an invoice or payable from start to finish without a system required approval by another individual.

Invoices and payables processed in SAP are then electronically transmitted to EnterpriseOne, the State's accounting system. Payments are made from EnterpriseOne via warrant or electronic funds transfer (EFT) the following day. Individuals with both SAP "MM_AP_MAINTAIN" and EnterpriseOne access can process an invoice or payable from start to finish on SAP and then approve the actual disbursement of the payment on EnterpriseOne the following day.

SAP Access as of April 2012 was as follows for the University of Nebraska-Lincoln (UNL), University of Nebraska Medical Center (UNMC), University of Nebraska at Omaha (UNO), University of Nebraska at Kearney (UNK), and University of Nebraska Central Administration (UNCA):

	UNMC	UNO	UNK	UNL	UNCA	Total
Individuals with Access to Process a Payable from Beginning to End in SAP	19	24	6	13	7	69
From those noted above, individuals with access to Enter Transactions on EnterpriseOne	4	7	5	5	6	27

SAP Access as of October 2012 was as follows:

	UNMC	UNO	UNK	UNL	UNCA	Total
Individuals with Access to Process a Payable from Beginning to End in SAP	14	24	6	14	5	63
From those noted above, individuals with access to Enter Transactions on EnterpriseOne	3	7	5	5	5	25

This was noted as a prior year finding.

Without adequate controls over the processing of transactions in the accounting systems, there is an increased risk of the loss or misuse of University funds.

> We recommend the University review access in SAP and EnterpriseOne when it involves Invoice/Payables and revise those roles to ensure that no one employee has access to enter, approve, and post an invoice or payable from beginning to end.

Management Response: The University disagrees that this is a significant deficiency as the magnitude of a potential misstatement resulting from this deficiency is small and the reasonable possibility that controls will fail to prevent, detect and correct a misstatement is low. The audit disclosed no misstatements of this nature.

In addition, the auditor does not acknowledge improvements made that buttress other internal controls already in place including the inability of a person to enter and park an invoice. We continue to assert that with at least two people involved in the payment of a single invoice, along with budgetary and other controls, there are mitigating controls present which greatly reduce the risk of fraudulent payments.

APA Response: AICPA Auditing Standards, AU Section 325.07, states "A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged

with governance." We believe this finding merits attention by the Board of Regents and is appropriately identified as a significant deficiency in compliance with auditing standards. Additionally AU Section 325.08, states for when evaluating the severity of deficiencies in internal control identified, "The severity of a deficiency does not depend on whether a misstatement actually occurred."

B. BASIC FINANCIAL STATEMENTS MANAGEMENT LETTER COMMENTS

2. Payroll Process

Our previous four audits noted some variation in the University payroll process at each of the campuses; however, the University's payroll process can generally be described as a negative reporting system. This means employees will be paid the same amount each pay period unless the Human Resources (HR) department receives information from the department head to change an employee's payroll. University departments generally do not document their review and approval that payroll is ready to be processed by central administration or their review of the "Payroll Expense Distribution Report by Cost Object" after payroll has been processed on SAP.

After payroll has processed, campus departments may have a report noting individual employees' payroll information sent to them for their review. However, there is no requirement for the department to respond back to the HR department that the payroll processed was accurate and complete. We recommended a payroll report be sent to all departments and that the report be reviewed and approved by appropriate department management/supervisors having knowledge of the completeness and accuracy of the department's payroll before payroll is processed and that these supervisors be required to respond to HR with their documented approval of payroll.
The University made no changes in the payroll process to address the above weakness and again responded to our prior year comment by indicating they understood our observation, but believed other controls present in the system provided many of the features sought in the recommendation. In addition, while the procedure suggested has merit, they believed it would require additional personnel and recordkeeping without providing a commensurate increase in controls.

A good internal control plan requires department management/supervisors document their review and approval of payroll reports.

Given the fact timesheets are not kept by many employees and there is no documentation that payroll was reviewed by supervisors; there is a greater risk of errors or irregularities occurring in the payroll process and going undetected.

> We again recommend a payroll report be sent to all departments and that this report be reviewed and approved by appropriate department management/supervisors having knowledge of the completeness and accuracy of the department's payroll before payroll is processed and that these supervisors be required to respond to HR with their documented approval of payroll.

Management Response: There are detective and budgetary controls in place which mitigate the risk of fraudulent personnel in the payroll system. Deans, directors, departmental chairs, and principal investigators review available reports and on-line comparisons of expense to budget during the year to assure expenses appear proper. The general ledger budget and expense comparisons augment other reports used by department chairs and managers to verify payroll expenses. These reports include the SAP Wage and Hour Report, the Budget Salary Balances Report, the Financial Information Detail Report, the Financial Information Payroll Cost Distribution, and the Revenue and Expense Summary with Carry-forward. The SAP Wage and Hour Report is used to review the payroll computations prior to payment. The suggestion by the APA of documenting the approval by each dean, director, and departmental manager in advance of paying a payroll with the veiled threat of withholding payroll if such documentation is not received, in practice, is impractical. The administrative burden and cost of creating the process suggested by the auditor will outweigh the additional control benefits gained.

APA Response: The University stated that deans, directors, departmental chairs, and principal investigators review available reports and on-line comparisons of expense to budget; however, these reviews are not always documented.

3. Outside Bank Account Activity

During FY 2012, the balance in University outside bank accounts exceeded 2% of the balance in University cash funds. Also, the Auditor of Public Accounts (APA) feels the activity in the accounts was excessive.

Neb. Rev. Stat. § 85-125 (Cum. Supp. 2012), § 85-192 (Cum. Supp. 2012), and § 85-1,123 (Cum. Supp. 2012) establish cash funds at UNL and UNMC, UNO, and UNK, respectively. These statutes all state the fund shall be in the custody of the State Treasurer, except that there may be retained by the Board of Regents, "a sum not to exceed two percent of the fund, which shall be available to make settlement and equitable adjustments to students entitled thereto, to carry on university activities contributing to the fund, and to provide for contingencies."

Neb. Rev. Stat. § 85-128 (Reissue 2008) states,

> *"The State Treasurer shall be the custodian of all the funds of the university. Disbursements from the funds named in sections 85-124 to 85-127 shall be made in accordance with the provisions of law relating to the disbursement of university funds in the hands of the State Treasurer as provided by law."*

During FY 2012, the APA noted the following activity at each of the University campuses:

	Credits	Debits
UNMC	$ 28,370,603	$ 28,768,318
UNO	$ 55,591,084	$ 55,663,111
UNL	$ 63,482,452	$ 63,846,300
UNK	$ 2,700,349	$ 2,726,595

The APA feels that the amount of activity in these outside bank accounts is excessive and more indicative of a depository account than an account for the settlement of operating expenses. The APA did note the campuses have established bank accounts under the State Treasurer to begin addressing these concerns and to determine the proper use of these accounts.

Additionally, the APA noted the following campuses exceeded two percent of the cash fund during these months in FY 2012.

Campus	Month	2% of Cash Fund (at month end)	Balance in Outside Accounts
UNO	July 2011	$ 484,080	$ 489,863
UNO	August 2011	$ 393,239	$ 1,311,223
UNO	September 2011	$ 497,684	$ 532,640
UNO	December 2011	$ 361,073	$ 400,306
UNO	May 2012	$ 511,564	$ 647,844
UNL	March 2012	$ 3,635,203	$ 4,574,533

We noted a similar finding in our prior year audit.

We believe the University is not in compliance with State statute in the way they use their outside bank accounts.

> We recommend the University continue to work with the State Treasurer to determine the correct use of their outside bank accounts. We also recommend the University develop policies and procedures to ensure that the balances in the outside bank accounts are in compliance with State statute.

Management Response: The University has worked with the State Treasurer to establish a separate bank account for each campus under the control of the Treasurer. These accounts were established during the third calendar quarter of 2012. Vendors, third parties, students, and other debtors are instructed to wire their payments to the appropriate campus account. Each campus is in the process of moving activity from their respective timely and equitable settlement account (petty cash) to their campus' State Treasury account. We anticipate these changes will be completed by June 30, 2013.

4. Group Health Trust Fund and Payroll Vendor Payments

Many years ago, the University established a Group Health Trust Fund (Trust Fund) to provide for the investment and administration of contributions made pursuant to the University's Health Insurance Program (Program). The University's Trust authorizes BCBSNE and Caremark, the Program's third party administrators, to withdraw – with little, if any, oversight – funds directly from the Trust Fund for the payment of claims. In fact, under that broad grant of authority, those third parties withdraw funds directly from the Trust Fund without either prior or subsequent University approval for each transaction.

On March 29, 2012, the APA issued an Attestation Report of the University of Nebraska Health Insurance Program. This finding was included in that report in significantly more detail than is included in this management letter. That report can be found on our website at **http://www.auditors.nebraska.gov/APA_Reports/2012/SA51-03292012-July_1_2009_through_June_30_2010_Health_Insurance_Program_Attestation_Report.pdf**.

Since 2003, the State of Nebraska (State) has utilized EnterpriseOne accounting software to record all of its official financial records in one centralized system. However, for more than a decade, the University of Nebraska (University) has relied upon its own separate software, Systems Applications and Products (SAP), which is then interfaced with EnterpriseOne, for accounting purposes.

Payroll vendor payments are set up differently in SAP than in EnterpriseOne. Payments made to vendors through the State's payroll process are recorded as vendor payments in EnterpriseOne. However, instead of generating vendor payments through SAP or EnterpriseOne during the payroll process, the University sends payroll payment instructions directly to the State's bank, authorizing the automatic deposit of payments to the vendors' banks. As a result, a vendor payment entry is not created in either accounting system; rather, a mere journal entry is made to record such payments. Because the University's accounting system does not record vendor payments to health insurance vendors, such as BCBSNE, the total amounts paid to these vendors cannot be determined or identified.

The following amounts were contributed by the employees and the University through the University payroll process between July 1, 2011, and June 30, 2012:

Contributions	**University**
Health and Dental Insurance*	$ 113,704,387
TIAA/CREF (Retirement)	$ 71,153,603
All other contributions	$ 72,354,546
Total	**$ 257,212,536**

*The employee health insurance plan is self-insured. Currently the University's health insurance contributions go into a separate bank account.

Sound accounting procedures include complete and accurate reporting of all payments to vendors to allow users of the State's accounting system to review and report on all vendor payments. According to Neb. Rev. Stat. § 81-1110.01 (Reissue 2008), the purpose of the accounting division of the Department of Administrative Services is:

> *"[T]o prescribe, coordinate, and administer a centralized, uniform state accounting and payroll system and personnel information system, to establish and enforce accounting policies and procedures for all state agencies, boards, and commissions, to monitor and enforce state expenditure limitations established by approved state appropriations and budget allotments, and to administer the federal Social Security Act for the state and the state's political subdivisions."*

When vendor payments do not originate from the State's accounting system, it is difficult for users of the system to ascertain the total amount paid to all vendors. This was noted as a finding in the prior two fiscal years' audits. The University indicated they explored the possibility of interfacing the payments from SAP to EnterpriseOne; however, they concluded to continue with their current practice.

Based upon both the relevant State statutes and the Attorney General's opinions noted in the APA's Attestation Report referenced above, the APA still questions the authority, statutory or otherwise, of the University to establish the Trust Fund outside of the custody and control of the State Treasurer. As of June 30, 2012, the Trust Fund had a balance of $143,617,630.

> We recommend that the University consult with the State Treasurer to resolve this issue and join with the State Treasurer in seeking, if needed, a formal opinion from the Attorney General as to the legality of the Trust Fund's existence outside the custody and control of the State Treasurer.
>
> We also recommend the University work with the Department of Administrative Services to develop a process that allows vendor payments to be accurately recorded in the State's accounting system.

Management Response: The University understands this comment pertains to the University's imprest payroll fund maintained in the Nebraska Information System (NIS) [EnterpriseOne]. All payroll salaries, benefits, and related payroll contributions and deductions are accounted for in the imprest fund. Payrolls are balanced for each biweekly and monthly payroll and at the end of the month. Charges and credits to the imprest fund are supported by electronic files and reports maintained by University. It is the University's belief adequate controls are in place to account for the imprest account activity in the NIS system.

C. INFORMATION TECHNOLOGY (IT) MANAGEMENT LETTER COMMENTS

5. NeSIS Security Breach

Generally Accepted Government Auditing Standards (GAGAS), 5.24 concerning the communication of significant matters in the Auditors' report states, in part,

> *"Examples of matters that auditors may communicate in a GAGAS audit include the following: b. Unusual or catastrophic events that will likely have a significant ongoing or future impact on the entity's financial condition or operations… d. Any other matter that the auditors consider significant for communication to users and oversight bodies in the auditors' report."*

On May 23, 2012, the University discovered a security breach had occurred in the University's Student Information System (NeSIS). On May 25, 2012, the breach was disclosed to the public. NeSIS contained approximately 21,000 bank account numbers and 650,000 social security numbers. On May 31, 2012, UNL police announced a UNL student was suspected in the attack on the NeSIS system. There was no evidence data was downloaded by the student.

On June 1, 2012, the Nebraska State College System announced the security breach also included the State College NeSIS environment, which was maintained by University IT staff. The State College environment did not house bank account information and there was no evidence that data was extracted from the system. The same UNL student was suspected of the attack.

When a data breach occurs, significant financial and personnel resources are used to investigate the incident, notify affected parties, pay for potential litigation and remedial actions, and mitigate the risk of future breaches. Public trust is also negatively affected when a security breach involving sensitive information is involved.

> We recommend the University continue to inform the public of information regarding the security breach as it becomes available and acceptable to be disclosed.

Management Response: The University takes its responsibility to inform the public very seriously and is pleased the APA agrees with actions taken. We will continue to inform the public of information regarding the security breach as it becomes available and acceptable to be disclosed.

6. Segregation of Duties – Awarding Financial Aid

A good internal control plan includes an adequate segregation of duties so that no one individual has the ability to create awards, configure award parameters, and apply awards to individual students.

During our audit, we noted 22 University staff have the ability to create scholarships in NeSIS, configure scholarship parameters, and also award scholarships to individual students. This included 10 UNMC, 7 UNL, and 5 UNCA staff (plus one system ID).

We noted a similar finding in our prior audit.

A lack of segregation of duties around the creation and application of scholarship awards increases the risk of a single individual setting up and applying awards to a student without another individual's knowledge.

> We recommend the University implement an adequate segregation of duties around the award process so no one individual is able to create a scholarship, configure the scholarship parameters, and then award the scholarship to students.

Management Response: The University agrees controls are necessary to prevent a student from being awarded more aid than they are eligible to receive. It is our belief those controls are in place. First, financial aid can only be awarded to students already in existence in the student information system and no financial aid employee can add a student to the system. Financial aid employees are not to take action on or award financial aid to students who are related or close friends that they have included on a disclosure statement. This activity is monitored by the management of the financial aid office. The campuses will also continue efforts to reduce the number of users who can both establish financial aid parameters and award financial aid as much as practical within budget constraints and the number of staff in the offices.

7. Waive Student Fees

A good internal control plan includes a periodic review of users access to ensure users are restricted to access which is required as part of their job function. A good internal control plan also includes a periodic review of fees waived to help determine if the amount of fees waived is reasonable.

During a review of user's access in NeSIS, we noted 44 UNO staff with the ability to waive various student fees in NeSIS. These individuals were primarily from the Records and Registration office, or cashiering/student accounts office. Half of the users were granted the access through the student records default role. The default role was widely used by registrar employees, contributing to the high number of users with the access. A limited number of registrar users required the access to waive 30-40 late registration fees per semester. The highest number of users with this access at any of the other University campuses was 11 (UNMC).

We noted a similar finding in our prior audit.

Allowing a large number of individuals to waive various student fees, increases the risk student fees could be inappropriately waived.

> We recommend UNO staff review the list of users with access to waive student fees to determine if they require the access for their daily job functions. For those users who do not require the access, we recommend their access be removed. We also recommend reviewing the access included in the student records default role to ensure it is reasonable.

Management Response: The UNO campus reviewed the users who had access to waive student fees. Based on the review, the number of users with access to waive student fees was reduced from 44 to 21 and the ability to waive fees was removed from the student records default role. A separate role was established for the waiver of student fees. The campus will continue to monitor the needs of those users granted the student fee waiver function and will make access changes as appropriate.

8. NeSIS SACR Security

The University's Student Information System (NeSIS) restricts user access in multiple ways. One way is to limit user access to data once they reach a page granted to them by a role; this is called SACR (Student Administration & Contributor Relations) security. For instance, the University can grant a user access to see student financial information by granting the user a specific role. Using SACR security, the University can then restrict an employee's access to a single campus (e.g. UNL). Without this additional SACR security setting, the employee would be able to see student financial information for all University students.

During a previous audit, we identified a portion of SACR security was turned off for NeSIS. The portion of security turned off secures the student financial information. As a result, adequate security layers were not active to prevent users from accessing some critical financial data at other campuses. It was also noted logging of SACR security changes were not recorded to allow the review of user access at the SACR security level. As of April 9, 2012, the University implemented this security in production.

Without adequate SACR security enabled, there is an increased risk a user will be able to access information, which is not essential to their job function. Without adequate logging of user access, the degree of a user's access cannot be adequately identified once the ID has been deleted. In cases of unauthorized access, there is an increased risk the University will be unable to adequately identify student records that could have been accessed.

> We recommend the University continue to fully utilize SACR security and restrict users access to the least privileges needed to perform their job function. We also recommend the University adequately capture the history of a user's access through documentation of SACR security applied to user profiles.

Management Response: SACR security was implemented in the NeSIS production system prior to the fiscal year end on April 9, 2012. The University will continue to fully utilize SACR security and restrict users access to the least privileges needed to perform their job function. We will further investigate and determine the best method to adequately capture the history of a user's access through documentation of SACR security applied to user profiles.

9. Password Parameters

Good business practices include establishing documented policies regarding minimum password standards that must be used by users to help adequately protect IT resources. A good internal control plan includes system enforced password parameters to ensure users meet minimum password standards.

IT Governance Institute's Objectives for Information and Related Technology (COBIT), Process Control 4.1, Policy, Plans and Procedures states,

> *"Define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training. Assign responsibilities for each of these activities and, at appropriate times, review whether they are executed correctly. Ensure that the policies, plans and procedures are accessible, correct, understood, and up to date."*

There was no enterprise-wide password policy in place to require consistent password complexity settings among all University campuses. Both SAP and NeSIS had password parameters and policies defined within various identity management systems, but did not appear to be reasonable or consistent based on other University and State government password policies in existence.

UNMC utilized their own management system to manage their password parameters; however, UNMC parameters were not consistent with TrueYou settings and did not appear to be reasonable based on other University and State government password policies in existence. The password parameters at UNMC were as follows: passwords had to be changed every 180 days; and users were not required to change their temporary passwords at their first login or after a reset.

We noted a similar finding in our prior audit.

When enterprise-wide policies are not established by management, there is an increased risk password parameters set by various University IT staff will not be sufficiently strong and in line with management's intentions. Strong password parameters are essential in providing adequate security to information systems and protecting internal data. Weak password parameters increases the risk unauthorized users may gain access to information systems and compromise the integrity and confidentiality of highly sensitive data.

> We recommend the University develop, approve, and publish minimum enterprise-wide password standards. We also recommend UNMC implement password settings that include requiring passwords to be changed at least every 90 days for all functional users, staff, and faculty. Finally, we recommend users be required to change their password upon first login or password reset.

Management Response: The University agrees password parameters have to be adequate to protect the system. A draft enterprise wide password policy has been developed. Approval of the policy will be sought from the appropriate management levels within the University structure.

10. NeSIS Terminated User Access

The University of Nebraska Executive Memorandum No. 16, Section 5, states "Unauthorized access to information systems is prohibited… When any user terminates his or her relation with the University of Nebraska, his or her ID and password shall be denied further access to University computing resources." A good internal control plan includes documentation of terminating users access through system audit records.

One University user with read access to PeopleTools Application Designer and inquiry access to all NeSIS pages had terminated on March 15, 2012, and still had access as of June 1, 2012. The user had both a named ID and a TrueYou ID still active in the system.

For 7 of 10 terminated University employees tested with NeSIS access, the APA was unable to determine if access was removed timely because the NeSIS audit log control established to record when a user's roles were added or removed was not functioning. For 2 of 10 University employees, the APA was able to identify NeSIS access was not removed within 3 business days following the termination. For 2 of 10 terminations, there was no documentation available to indicate an appropriate staff member had been notified to remove the terminated employee's access.

Employee	Campus	Audit Log Available	Access Removed Timely
1	UNMC	No	?
2	UNL	No	?
3	UNK	No	?
4	UNL	No	?
5	UNMC	Yes	Yes
6	UNO	No	No
7	UNK	Yes	Yes
8	UNMC	Yes	No
9	UNO	No	?
10	UNL	No	?

For the UNK termination tested, a dynamic role process did not function properly, as it added back roles to the user profile of the terminated individual once they were removed. UNL staff used a monthly process for identifying and removing terminated users. This process allowed terminated users to retain NeSIS access for up to 30 days after their termination.

We noted a similar finding in our prior audit.

When a user's access to IT systems is not terminated timely, there is an increased risk business processes will be negatively impacted due to terminated employees accessing critical resources. When IT controls do not function in accordance with management intentions, there is no support to verify staff is removing terminated employees in a timely manner.

We recommend the University develop a formal system wide process to ensure appropriate staff is notified of all terminations in order to remove NeSIS access within a reasonable period of time. The creation, modification, and removal of a user's access should be documented and include a date stamp. We also recommend system audit logs be properly maintained.

Management Response: The NeSIS support team will work with the campuses to develop a formal, system wide process for the removal, documentation and time stamped log of terminated staff from the NeSIS system.

11. Mainframe Settings and User Management

The University of Nebraska Executive Memorandum No. 16, Section 5, states "Unauthorized access to information systems is prohibited… When any user terminates his or her relation with the University of Nebraska, his or her ID and password shall be denied further access to University computing resources." A good internal control plan also includes procedures to remove access timely when users transfer job functions or no longer require access to perform their job function.
We identified 11 users with elevated access who had not logged in for over one year. Two of the users had terminated; however, their IDs were not removed or revoked upon termination. User profiles were revoked after 90 days of inactivity.

We noted a similar finding in our prior audit.

When users, who no longer require access, are not identified and removed in a timely manner, there is an increased risk of sensitive data being attained or valuable resources utilized.

We recommend the University implement procedures to remove access timely for those individuals who no longer need such access, including terminated users.

Management Response: The Computer Systems Network (CSN) reduced the number of inactive days from 255 to 90 for the removal of inactive users from mainframe access during the year. CSN will continue to work with the campuses to determine options to further reduce the time period for the removal of inactive or terminated users.

12. SAP Change Management

A good internal control plan includes a change management process that is performed by multiple individuals and is documented from start to finish.

We identified two individuals with access to complete the entire change management process. For 1 of 25 SAP changes tested, the change request form was completed by a single individual. Changes made through the formal process, using change request forms, were not reviewed when the change was performed by one individual.

We noted a similar finding in our prior audit.

Allowing a single person to develop, approve, and promote a change to SAP without review, increases the risk a change to the SAP application could be made in contrast to management's intentions.

> We recommend the University have a staff member, with knowledge of approved changes to SAP, perform and document his/her review of changes promoted to production. This employee should not be able to complete all aspects of a change.

Management Response: The current change control process and software does not easily allow this segregation capability. Newer, integrated software may support segregating the change control steps and will be evaluated during the year.

* * * * *

This letter is intended solely for the information and use of management, the Board of Regents of the University of Nebraska, others within the University, Federal awarding agencies, and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties. However, this letter is a matter of public record and its distribution is not limited.

Sincerely,

SIGNED ORIGINAL ON FILE

Mark Avery, CPA
Audit Manager