The University of Nebraska

Management Letter

For the Year Ended June 30, 2019

Issued on February 10, 2020

NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

Charlie.Janssen@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
auditors.nebraska.gov

December 13, 2019

The Board of Regents
University of Nebraska

We have audited the financial statements of the University of Nebraska (University), a component unit of the State of Nebraska, for the year ended June 30, 2019, and have issued our report thereon dated December 13, 2019.

Our audit procedures were designed primarily to enable us to form an opinion on the Basic Financial Statements. Our audit procedures were also designed to enable us to report on 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 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.

The following is a summary of our Report on 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*. Our complete report can be found with our report on the financial statements of the University dated December 13, 2019.

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the business-type activities, and the discretely presented component unit of the University as of and for the year ended June 30, 2019, and the related notes to the financial statements, which collectively comprise the University's basic financial statements, and have issued our report thereon dated December 13, 2019. Our report includes a reference to other auditors who audited the financial statements of the University of Nebraska Foundation (Foundation), a discretely presented component unit of the University; the University of Nebraska Facilities Corporation, the University Technology Development Corporation, the University Dental Associates, the UNeHealth, the UNMC Science Research Fund, and the Nebraska Utility Corporation, blended component units of the University (collectively identified as the Blended Component Units); and the activity relating to the Members of the Obligated Group Under the Master Trust Indenture, as described in our report on the University's financial statements. The financial statements of the Foundation, the University of Nebraska Facilities Corporation, the University Dental Associates, the UNeHealth, the UNMC Science Research Fund, and the Nebraska Utility Corporation were not audited in accordance with *Government Auditing Standards* and, accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with these entities.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances 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. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

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. 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.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free from 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 did note certain other matters that we reported to management included in the following Schedule of Findings and Responses.

University's Response to Findings

The University's responses to our findings are described below. The University's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

SCHEDULE OF FINDINGS AND RESPONSES

1. Audit Differences

A good internal control plan and sound accounting practices require financial information to be complete and accurate. This includes procedures to ensure the financial statements are correct, and adjustments are made to rectify all known significant ($1,000,000 or more) misstatements.

During our audit of the financial statements, we noted errors that resulted in significant misstatements. We proposed the University adjust its statements to correct all of these errors. The University did adjust the statements for all corrections proposed.

The following are significant misstatements the University corrected:

- The University Technology Development Corporation (UTDC) reported grants and contracts revenue of $19,761,000 and $12,643,000 for the fiscal years ended June 30, 2019, and June 30, 2018, respectively. When the University blended UTDC into its financial statements, it classified these entire amounts as private grants and contracts – restricted revenue. However, $18,455,000 in fiscal year 2019 and $12,145,000 in fiscal year 2018 revenue should have been classified as Federal grants and contracts – restricted revenue, as the revenue came from Federal sources.

- All University campuses collected technology fees during the fiscal years ended June 30, 2019, and June 30, 2018. The University of Nebraska-Omaha (UNO) classified technology fees of $1,826,443 for fiscal year 2019 and $2,073,509 for fiscal year 2018 as sales and services of educational activities revenue. This was inconsistent with other campuses, all of which classified technology fees as tuition and fees revenue.

- UNO improperly classified $3,169,000 in fiscal year ended June 30, 2019, cash flows on its Statement of Cash Flows as a cash inflow from sales and services of auxiliary operations. However, as the cash flow was from capital grants and gifts, it should have been classified as a cash inflow from capital grants and gifts.

- The University of Nebraska-Medical Center (UNMC) did not include a donated building valued at $36,000,000 on its Statement of Cash Flows. It should have been reflected as a non-cash capital gift and grant in the Non-Cash Transactions section of the Statement.

- For the fiscal year ended June 30, 2019, the University revised its method for pulling in the University of Nebraska Facilities Corporation (UNFC) cash flows into the Statement of Cash Flows. However, it did not restate its fiscal year 2018 amounts for comparability. This resulted in two amounts being misstated in the Reconciliation of Operating Loss to Net Cash Flows from Operating Activities section of the Statement of Cash Flows. The adjustment for Other Current Assets was overstated by $14,271,000, while Accounts Payable was understated by the same amount.

- UNMC recorded monies due from the National Strategic Research Institute (NSRI), which is a subsidiary of UTDC, at June 30, 2019, as both a due from and an accounts receivable (A/R), which resulted in revenue being double recorded and an A/R being improperly recorded. To eliminate

the A/R and double-recorded revenue, UNMC should have posted an entry to debit the revenue and credit the A/R. Instead, it posted an entry that debited revenue and credited deferred revenue. This resulted in both A/R and deferred revenue being overstated by $2,015,369.

Without strong internal control procedures and accounting practices to ensure financial information is complete, accurate, and in accordance with accounting standards, there is a greater risk material misstatements may occur and remain undetected.

A similar finding was noted in our prior audits.

> We recommend the University implement procedures to ensure financial information is complete, accurate, and in accordance with accounting standards.

Management Response: *The University strives to present financial statements accurately and in accordance with generally accepted accounting principles as prescribed by the Governmental Accounting Standards Board (GASB). We will continue to explore additional review processes, but at this point there does not seem to be a significant return on the application of additional resources.*

2. General Ledger Transactions in SAP

The workflow in the SAP system does not require separate preparers and posters of General Ledger (GL) type transactions, primarily journal entries that do not result in vendor payments. As a result, certain individuals throughout the University had the capability of completing GL transactions from beginning to end without a documented secondary review and approval in SAP. The University did have a policy in place to review any journal entries (JE), payroll journal entries (PJ), NIS (refers to E1) journal entries (ND), University-only journal entries (UU), and non-Federal ACH receipt (CN) transactions over $49,999, or $499 when involving Federal funds, to address this inherent system weakness.

During our audit of the GL security roles in SAP, we identified 546 users with the ability to prepare and post GL entries in SAP without a system-required secondary review or approval. The 546 users are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	266
UNMC	225
UNO	33
UNCA	17

(Document Types: JE – Journal Entry, IB – Internal Charges Batch, and IC – Internal Charges Online)

A secondary role allowed 79 of those users to prepare and post additional GL document types. The 79 are noted by location below, along with the GL document types they could prepare and post:

Campus	# of Users
UNK	5
UNL	30
UNMC	22
UNO	13
UNCA	9

(Document Types: CN – ACH Receipt, ND – NIS Journal Entry, UU – University Only Journal Entry, UA – Accrual Journal Entry, TN – Interstate Billing Transaction, and PJ – Payroll Journal Entry)*

**NIS refers to the State's EnterpriseOne accounting system.*

A good internal control plan requires a proper segregation of duties to ensure no one individual can process a transaction from beginning to end. A good internal control plan also includes adequate security controls, through the design, creation, approval, and assignment of user roles, to prevent users from performing functions that do not allow for a proper segregation of duties.

When individuals are able to complete GL transactions without a system-required secondary review or approval prior to posting the transaction to the GL, there is a greater risk for error and inappropriate GL transactions to occur and remain undetected. Additionally, in the absence of an adequate segregation of duties, there is an increased risk of loss, theft, or misuse of funds.

A similar finding was noted in our prior audits.

> We recognize that the University has a policy to review higher-risk general ledger transactions to mitigate risks related to the SAP system not having an established workflow, which would automatically require a segregation of duties in the preparation and posting of general ledger entries. Nevertheless, we continue to recommend that the University modify its role configuration for the 546 users identified, so that those users will not have the ability to post any GL transaction types in SAP without a system-required secondary review or approval.

Management Response: *The University conducted a cost/benefit analysis of implementing workflow within the SAP system to require review and approval of general ledger entries by a secondary approver. Given the significant estimated cost that would be required to implement workflow, we determined implementation is not justified at this time. We will continue our policy to review higher-risk general ledger transactions as a mitigating control.*

3. Contracts Not on the State Contracts Database

During testing of 76 expenditures governed by contracts, 11 contracts and/or amendments were not included on the State Contracts Database, as required by State statute. The contracts and/or amendments not included on the State Contracts Database were one at UNCA, two at UNK, one at UNL, four at UNMC, and three at UNO.

Neb. Rev. Stat. § 84-602.04(4)(a)(i) (Cum. Supp. 2018) requires the Department of Administrative Services' web site to contain the following:

> *A data base that includes a copy of each active contract that is a basis for an expenditure of state funds, including any amendment to such contract and any document incorporated by reference in such contract. For purposes of this subdivision, amendment means an agreement to modify a contract which has been reduced to writing and signed by each party to the contract, an agreement to extend the duration of a contract, or an agreement to renew a contract. The data base shall be accessible by the public and searchable by vendor, by state entity, and by dollar amount. All state entities shall provide to the Department of Administrative Services, in electronic form, copies of such contracts for inclusion in the data base beginning with contracts that are active on and after January 1, 2014 . . . .*

A similar finding was noted in our prior audits.

> We recommend the University include all of its contracts on the State Contracts Database in a timely manner to comply with State statute.

Management Response: *The University will strive to continue filing contracts in the State Contracts Database on a timely basis. In addition, Internal Audit & Advisory Services will continue testing.*

4. University Password Settings

The University's Identity Management system, known as SailPoint, is used for setting a global password policy. In addition, the University also establishes password settings and authenticates to SAP through a central active directory. UNK, UNL, and UNO also use the central active directory to authenticate to the Nebraska Student Information System (NeSIS). UNMC uses a separate active directory to authenticate to NeSIS.

During our review of the University's password settings in SailPoint and the central active directory, we noted the following settings were not in compliance with the National Institute of Standards and Technology (NIST) Digital Identity Guidelines:

- Users are allowed to select prompts from a set of six questions and to reset their password by providing answers to three of those questions, generated randomly.

- The University passwords that are stored in SailPoint were not salted and hashed, which is a method of encryption.

- The University re-authentication settings for SAP and NeSIS were inadequate. Users were not required to re-authenticate to SAP and NeSIS until after 9 and 12 hours of inactivity, respectively.

During our review of UNMC's password settings in its active directory, we noted the active directory does not compare user passwords against a list of values known to be commonly used, expected, or compromised.

The University's Password Policy, Version 1.1 (Revised March 4, 2014), states the following:

> *Any credential which identifies a subject or service account should follow recommendations outlined in National Institute of Standards (NIST) 800-63-2 [2], [3] using a token method and the level of entropy or randomness as outlined in §§ 6.1.2 and 6.3.*

NIST has since issued Special Publication (SP) 800-63-3 in June 2017, which supersedes NIST SP 800-63-2. Additionally, SP 800-63-3, SP 800-63A, SP800-63B, and SP 800-63C provide technical guidance to agencies for the implementation of digital authentication.

NIST SP 800-63B (June 2017), § 5.1.1.2, states, in relevant part, the following:

> *Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets. When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised . . . . Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function. Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.*

NIST SP 800-63B (June 2017), § 4.2.3, states, in relevant part the following:

> *Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.*

Good internal control includes system-enforced password parameters to ensure users meet minimum password standards. Inadequate password settings increase the risk of unauthorized users gaining access to sensitive information contained in both the NeSIS and SAP applications.

A similar finding was noted in our prior audits.

> We recommend the University strengthen its password parameters to achieve compliance with NIST standards.

Management Response: *The University of Nebraska and Nebraska State College System continue to expand adoption of two-factor authentication to mitigate the risk of single-factor memorized secrets. The University is revising its password policy and implementing technical changes to align with the latest recommendations in NIST 800-63-3.*

All passwords stored within the SailPoint Identity Management system are encrypted using AES 128 bit keys, and this is needed to provision the multiple Active Directory accounts needed for authentication. The University is working to consolidate authentication stores and once this is complete will be able to remove the encrypted passwords, leaving only the hashed passwords in the single Active Directory.

The University will work to adjust session lengths and re-authentication timeouts based on the different Authenticator Assurance Levels.

5. User Terminations

For 4 of 25 SAP terminated users tested, access was not removed within three business days of the employees' last working date. The time it took to remove access ranged from 6 to 108 business days. The four users with access not removed timely included two at UNL, one at UNMC, and one at UNO.

For 3 of 25 NeSIS terminated users tested, access was not removed within three business days of the employees' last working date. The time it took to remove access ranged from 7 to 41 business days. The three users with access not removed timely included one each at UNL, UNMC, and UNO. For all three of these users, there was a discrepancy between the employee's last working date in the office and the

employee's official termination date recorded in SAP. Additionally, we reviewed SAP access for these three users and noted that their SAP access was not removed timely as well. The time it took to remove their SAP access ranged from 7 to 40 business days.

Additionally, during our testing of users with NeSIS SACR access, we noted that a terminated UNMC temporary employee had SACR access. The University removed her access after the APA made it aware of the issue. Access was removed 102 business days after her termination.

The University of Nebraska Executive Memorandum No. 16 (Section 5) states the following:

> *Unauthorized access to information systems is prohibited . . . . When any users 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.*

InCommon Identity Assurance Profiles: Bronze & Silver (February 11, 2013), Section 4.2.4.2, states, "The IdPO shall revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised." Human resource staff are responsible for notifying the Identity Provider (IdPO) of terminations and should work to achieve access removal within a 72-hour period.

A good internal control plan requires terminated user access to be removed timely and documentation, whether by system audit records or access removal forms, or both, be available to indicate that such access was removed properly.

> We recommend the University implement a formal procedure at each campus to ensure the appropriate staff is notified of all terminations in order to remove NeSIS and SAP access within three business days and that this procedure be documented. We recommend the process include entering termination dates – when they are known – in SAP prior to the actual termination.

Management Response: *Both NeSIS and NeBIS have reviewed the terminated users with elevated access and the elevated access has been removed. Management will work with the NeBIS team and the campuses to improve our user termination business practices, procedures and policies.*

6. Change Management

During change management testing, we noted that several SAP and NeSIS application changes were not documented and approved in accordance with the University Change Control Policy (IT-02).

The University Change Control Policy (IT-02) was approved by the University's president on April 17, 2017. Section II of IT-02 states the following, in relevant part, the following:

> *All changes to information systems (hardware and software) and networking components or architecture should follow a change management process. These changes include developing, testing, deploying, and maintaining systems and services, as well as all forms of change that may impact the physical location, configuration, and administration of assets associated with the computing and networking environments.*

Section III(A) of IT-02 lists various responsibilities of system owners or system administrators, including "Approval of the Change Request by the Change Advisory Board." However, the Change Advisory Board (CAB) did not begin approving SAP changes until September 2018, and NeSIS changes were not approved until October 2018. As a result of the CAB not approving changes until September and October 2018, 9 of 22 SAP changes and 11 of 25 NeSIS changes we tested were not approved by the CAB.

Another responsibility of system owners or system administration listed in Section III(A) of IT-02 is Completion of a Change Request Form. Information Technology Services (ITS) implemented a Request for Change (RFC) form to standardize the change management documentation process. The SAP team indicated that they adopted the RFC process in September 2018. However, during testing we noted that 6 of 19 SAP changes tested that were implemented after this date were not documented on an RFC form. The NeSIS team indicated that they adopted the RFC process in October 2018. However, during testing we noted that 1 of 15 NeSIS changes tested that were implemented after this date were not documented on an RFC form.

The SAP and NeSIS teams considered several of the changes we tested out of the scope of IT-02. One such change was an emergency change for which the NeSIS team did not obtain CAB approval. However, Section III(B) of IT-02 states, "The normal change management request process will be followed by completing a system change request documenting the need for an emergency change."

To clarify what types of changes were within the scope of IT-02, ITS issued multiple procedure documents during 2019. These documents also provided that the business or ITS representative who initiates a request for change is responsible for completing the RFC form and ensuring proper approval is obtained for the change. During testing, we noted that changes completed subsequent to the approval of these documents were properly documented and approved by the CAB, when required.

When IT change control policies are not clearly stated and communicated effectively, there is increased risk that the system owners will not comply with the policy.

> We recommend the University ensure its IT policies are clearly stated and effectively communicated. We further recommend system owners implement procedures to ensure changes are properly documented and approved, as required by IT policies and procedures.

Management Response: *University of Nebraska Information Technology Services (ITS) is responsible for the change control process and has procedures in place to comply with IT-02. These procedures have been amended as the process is solidified, and NeSIS and NeBIS have worked with ITS to ensure changes are submitted/approved according to the policy and procedures.*

7. NeSIS Business Continuity Planning

The University has not completed periodic testing of its process to restore NeSIS to functionality at its backup site in the event the application fails at its main location. The University indicated it has not completed a full failover test of NeSIS from its main location to its backup site since September 2015. Additionally, the University did not document the test.

COBIT 2019 Framework, Governance and Management Objectives, DSS04.02 Maintain business resilience, states, in part, the following:

> *Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption . . . .*
>
> 1. *Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.*
> 2. *Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption would have on them.*

3. *Establish the minimum time required to recover a business process and supporting I&T, based on an acceptable length of business interruption and maximum tolerable outage.*

4. *Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.*

5. *Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.*

6. *Analyze continuity requirements to identify possible strategic business and technical options.*

7. *Identify resource requirements and costs for each strategic technical option and make strategic recommendations.*

8. *Obtain executive business approval for selected strategic options.*

COBIT 2019 Framework, Governance and Management Objectives, DSS04.03 Develop and implement a business continuity response, states, in part, the following:

Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident . . . .

* * * *

3. *Define the conditions and recovery procedures that would enable resumption of business processing. Include updating and reconciliation of information databases to preserve information integrity.*

COBIT 2019 Framework, Governance and Management Objectives, DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP), states, in part, the following:

Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed . . . .

1. *Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP and DRP in meeting business risk.*

2. *Define and agree on stakeholder exercises that are realistic and validate continuity procedures. Include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.*

3. *Assign roles and responsibilities for performing continuity plan exercises and tests.*

4. *Schedule exercises and test activities as defined in the continuity plans.*

5. *Conduct a post-exercise debriefing and analysis to consider the achievement.*

6. *Based on the results of the review, develop recommendations for improving the current continuity plans.*

Good internal control requires procedures/hardware to be thoroughly tested to ensure the timely resumption of business processing in the event of application disruption or failure.

When processes intended to be used in the event of critical application failure or disaster have not been thoroughly tested, there is an increased risk of prolonged discontinuation of government processes in the event of application disruption or failure.

We recommend the University complete periodic documented testing of its NeSIS failover process to ensure continuity of operations for the NeSIS application in the event of application disruption or disaster.

Management Response: *University of Nebraska Information Technology Services (ITS) is responsible for the Disaster Recovery (DR) planning of the NeSIS system. While Business Continuity Planning is the responsibility of our customer base, ITS does include functional (business) testing within our DR exercises to ensure data integrity and business processing is tested and approved.*

A live exercise of the NeSIS system was performed on Jan 2, 2020 utilizing a full copy of the Production environment data recovered to the Quality environment. The objectives of that exercise were:

- *Identify and document minimum critical server environment requirements to operate production environment at our alternate location*
- *Identify and document system configuration changes required to operate production environment at our alternate location*
- *Establish and document communication channels and roles between technical staff, functional staff, and the Incident Management channel*
- *Document sequence of steps and dependencies necessary to recover at our alternate location including key decision points, communication check points, and testing check points*
- *Identify testing scenarios both at the technical and functional level that should be performed before start-up of our production environment at our alternate location*
- *Document the duration of each task of the recovery effort to begin business impact discussions with our customers*

* * * * *

It should be noted that this letter is critical in nature, as it contains only our comments and recommendations on the areas noted for improvement and does not include our observations on any strengths of the University.

Draft copies of this management letter were furnished to the University administrators to provide them with an opportunity to review and respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this management letter. Such responses have been objectively evaluated and recognized, as appropriate, in the management letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

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, and the appropriate Federal and regulatory awarding agencies and pass-through entities, and it is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,

Mark Avery, CPA
Assistant Deputy Auditor