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
www.auditors.nebraska.gov

May 22, 2017

Byron Diamond, Director
Department of Administrative Services
1526 K Street, Suite 240
Lincoln, NE 68508

Dear Mr. Diamond:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265, which permits the early communication of audit findings due to their significance and the need for corrective action. The work addressed herein was performed as part of the fiscal year ended June 30, 2017, Comprehensive Annual Financial Report (CAFR) audit. This communication is based on our audit procedures and related activity through April 30, 2017. Because we have not completed our audit of the fiscal year 2017 CAFR, additional matters may be identified and communicated in our final reports.

In planning and performing our audits of the State's financial statements, the Auditor of Public Accounts (APA) considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures. The audit procedures selected were utilized for the purpose of expressing our opinions on the financial statements of the State, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. However, has discussed below, we identified a certain deficiency in internal control that we consider to be a significant deficiency.

We noted a certain internal control or compliance matter related to the activities of the Department of Administrative Services (DAS) or other operational matters, which is presented below for your consideration. The following comment and recommendation, which has been discussed with the appropriate members of DAS and its management, is intended to improve internal control or result in other operating efficiencies.

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. We did not identify any deficiencies in internal control that we consider to be material weaknesses.

A significant deficiency is a deficiency, or 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 consider Comment Number 1 (EnterpriseOne Business Continuity Planning) to be a significant deficiency.

Draft copies of this letter were furnished to DAS to provide its management with an opportunity to review and to respond to the comment and recommendation contained herein. Any formal response received has been incorporated into this letter. Such response has been objectively evaluated and recognized, as appropriate, in the letter. A response that indicates corrective action has been taken was not verified at this time, but it will be verified in the next audit.

The following is our comment and recommendation relating to EnterpriseOne business continuity planning.

1. EnterpriseOne Business Continuity Planning

In the prior year, we noted that DAS had hardware in place, an IBM Power Systems Capacity BackUp (CBU), in case there should be a failure of EnterpriseOne (E1), the State's accounting system. However, that hardware had not been completely set up or thoroughly tested. According to DAS, the CBU was set up for data replication but not as a failover system. A failover system would ensure the E1 application could be switched over to redundant or standby equipment (and business could be continued as usual) in the event of disruption or failure of the E1 production environment. DAS stated that, even in a best case scenario, it would take days to get the E1 application up and running using the CBU. Additionally, DAS explained that the E1 application could run off the CBU for only a short time (approximately 30 days), and other hardware would need to be set up to take over for the CBU. Accordingly, the DAS E1 business continuity plan lacked procedures that would enable a timely resumption of business processing in the event of E1 disruption or failure.

During the fiscal year, E1 hardware for all environments and the CBU were replaced. Additionally, the disaster recovery site was moved from a University of Nebraska datacenter to a new location operated under an interlocal agreement between the City of Omaha and Douglas County. Attempts to bring the E1 environments onto the same network as the CBU have failed. As a result, replication of E1 data to the disaster recovery site has not been occurring since December 2016. Extensive effort to diagnose the cause of network errors preventing replication on the new network has not been successful.

It was noted that a full tape backup of E1 is completed weekly, and incremental backups are completed daily. Those tape backups are picked up for offsite storage daily. As the disaster recovery site is not currently capable of hosting E1 in the event of a significant disruption or disaster, an even more significant amount of downtime would likely ensue as a new site and hardware were obtained, hardware and network configured, software installed, data loaded from tape, interfaces configured, etc.

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), Section 1, Standard, states, in part, the following:

Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.

COBIT 5, a business framework for the governance and management of enterprise information technology, DSS04.02 Maintain a continuity strategy, states, in part, the following:

Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure enterprise recovery and continuity in the face of a disaster or other major incident or disruption . . . . 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 IT based on an acceptable length of business interruption and maximum tolerable outage . . . . 5. Analyze continuity requirements to identify the possible strategic business and technical options . . . . 8. Identify resource requirements and costs for each strategic technical option and make strategic recommendations. 9. Obtain executive business approval for selected strategic options.

COBIT 5, DSS04.03 Develop and implement a business continuity response, states, in part, the following:

Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the enterprise to continue its critical activities . . . . 4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity . . . .

COBIT, DSS04.04 Exercise, test and review the BCP, states, in part, the following:

Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.

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

When real-time data replication is not performed, and the disaster recovery site is not capable of hosting the accounting system, there is a significant risk of prolonged discontinuation of government processes in the event of application disruption or failure. Additionally, when hardware intended to be used in the event of critical application failure or disaster has not been completely set up and thoroughly tested, there is an increased risk of prolonged discontinuation of government processes in the event of application disruption or failure.

We recommend DAS resolve network issues at the disaster recovery site and implement effective business continuity controls, including adequate set up and testing of existing hardware or purchased hardware/services, to ensure continuity of operations for its E1 application in the event of application disruption or disaster.

Department Response: DAS leadership concurs that the EnterpriseOne system still does not have adequate disaster recovery hardware, software, processes, and procedures in place to ensure a real time cutover from the current production environment to a recovery environment. We are continuing to work with the OCIO to establish and expand these capabilities to first, be able to conduct real time replication of the core mainframe data and infrastructure of the state's financial system of record between the 501 building data center and the DOT.COM data center located in Omaha, NE. Once this capability is reached later this year, we will then work on building out the web server infrastructure to eventually create a dual recovery environment in Omaha.

The long-term solution will be in place within the next two to three years when the state completes its migration to the, yet to be selected; cloud-based environment where our data of record will be replicated and maintained in four geographically dispersed data centers across the United States. This disaster recovery capability will be provided as part of our cloud subscription services with our future vendor.

* * * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of DAS and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to DAS.

This interim communication is intended solely for the information and use of DAS, its management, the Governor and the State Legislature, and others within these State agencies. It is not intended to be, and should not be, used by anyone other than the specified parties. However, this letter is a matter of public record, and its distribution is not limited.

If you have any questions regarding the above information, please contact our office.

Sincerely,

Philip J. Olsen, CPA CISA
Audit Manager