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

January 29, 2016

Matt Blomstedt, Commissioner of Education
Department of Education
301 Centennial Mall South, 6th Floor
Lincoln, Nebraska 68509

Dear Mr. Blomstedt:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Nebraska (State) as of and for the year ended June 30, 2015, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, we have issued our report thereon dated December 17, 2015. In planning and performing our audit, we considered the State's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances 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.

In connection with our audit described above, we noted certain internal control or compliance matters related to the activities of the Department of Education (Agency) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the Agency's management, are intended to improve internal control or result in other operating efficiencies.

Our consideration of internal control included a review of prior year comments and recommendations. To the extent the situations that prompted the recommendations in the prior year still exist, they have been incorporated in the comments presented for the current year. All other prior year comments and recommendations (if applicable) have been satisfactorily resolved.

Our consideration of internal control was for the limited purpose described in the first paragraph 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 or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

In addition, we noted other matters involving internal control and its operation that we have reported to management of the Agency in a separate early communication letter pursuant to AICPA Auditing Standards AU-C Section 265.A17, dated July 20, 2015.

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

The following are our comments and recommendations for the year ended June 30, 2015.

1. Application Developer Access to Production Environment

Nebraska Information Technology Commission (NITC) NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.3.2.3, Separation of Duties, states the following:

> *To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.*

A good internal control plan includes restricting access to information resources based upon job responsibilities to help enforce a proper segregation of duties and reduce the risk of unauthorized system access. Programmers should generally be limited to accessing only the information specifically required to complete their assigned system development projects, as well as be expressly prohibited from altering production data and production software.

The Disability Determination System (DDS) serves as a customer resource manager and information tracking system for payments to medical practitioners for information they provide to the social security administration pertaining to pending disability claims.

Two DDS application developers and one DDS contract developer had full access to the production environment. Application developers with access to the database and the production environment have the ability to circumvent the standard change control process and implement modifications that may be inconsistent with management's intentions, which could result in unauthorized changes to data.

A similar finding was noted during the previous two audits.

> We recommend the Agency implement controls to ensure application changes are approved and documented. This includes implementing a segregation of duties in the change management process when migrating changes to production environments. If a segregation of duties cannot be maintained due to staff size, we recommend implementing compensating controls. Compensating controls may include reviewing audit logs, code changes, or automatic notifications by someone other than the developer(s) to identify all changes made to the production environment.

Agency Response: DDS Administrative staff have implemented controls to ensure application changes are approved and documented. The IT Supervisor will document all requested changes with an email to IT staff and a return email will be sent by IT staff to the IT Supervisor upon completion of the requested change. The emails will be maintained in an electronic folder to document the process.

2. Application Change Management and User Access

NITC Standards & Guidelines, Information Security Policy 8-101, Section 4.9.11, Change Control Management, states the following, in relevant part:

> *To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained. These change control procedures will apply to agency business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.*

A sound business practice includes maintaining documentation to support who requested, developed, tested, and approved a change in order for the change to be promoted to production.

The QE2 application is utilized by Vocational Rehabilitation staff to track expenses paid to assist physically and/or mentally disabled persons in locating jobs. It includes aid to complete school, assistance to purchase dress clothes, assistance to set up interviews, etc. The Agency uses the Redmine application to document the change management process for QE2.

The Agency made 63 changes to the QE2 application during the fiscal year ended June 30, 2015. We selected 10 changes and tested for documentation of when and by whom the changes were requested, tested, and approved. For nine changes there was no documentation of approval. We also noted five changes had no documentation they were tested.

When the testing and approval of a change to an application is not documented, there is an increased risk a change could be developed and promoted to production that is not in agreement with management's intentions.

A similar finding was noted during the previous audit.

> We recommend the Agency implement procedures to document adequately all steps of a change to applications, including when and by whom the change was requested, tested, approved, and promoted to production.

Agency Response: As reported in the IT Audit, Redmine is used to document the steps of a change for applications. VR will look to add an additional benchmark in Redmine to document the approval step. If that is not feasible, approval of deployment will be done via an email message and attached as a document to the case in Redmine. We will also explore adding categories for "tested by" and "deployed by" to simplify documentation of all steps.

3. Risk Assessment

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.5.1, Physical Security Perimeter, states the following, in relevant part:

> *Agencies will perform a periodic threat and risk assessment to determine the security risks to facilities that contain State information . . . .*

NITC Standards and Guidelines, Information Security Policy 8-101, Section 4.9.3, Risk Assessment, states the following:

> *Security requirements and controls must reflect the value of the information involved, and the potential damage that might result from a failure or absence of security measures . . . . The framework for analyzing the security requirements and identifying controls to meet them is associated with a risk assessment, which must be performed by the data owner(s) and Agency management. A process must be established and implemented for each application to:*
>
> - *address the business risks and develop a data classification profile to understand the risks;*
> - *identify security measures based on the criticality and data sensitivity and protection requirements;*
> - *identify and implement specific controls based on security requirements and technical architecture;*
> - *implement a method to test the effectiveness of the security controls; and*
> - *identify processes and standards to support changes, ongoing management and to measure compliance.*

A good internal control plan requires a risk assessment to be completed and updated periodically.

During the prior audit, the Agency performed some risk assessment activities but lacked a formalized risk assessment plan for all applications. During the current audit, we noted the Agency prepared a risk assessment report; however, it lacked application-specific risk information. The Agency has multiple applications, which may have different levels of risk.

When risk assessments lack application-specific information, there is a possibility that an application risk will not be identified. This could increase the probability of security vulnerabilities that could have been prevented or monitored being exploited, causing such issues as downtime, loss of productivity, unauthorized access, or interference with State or Federal systems.

> We recommend the Agency improve its risk assessment by including application-specific risk information.

* * * * *

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 the Agency 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 the Agency.

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

Don Dunlap, CPA
Assistant Deputy Auditor