



Douglas County Internal Audit

September 7, 2012

Douglas County Board of Commissioners
1819 Farnam Street, Suite LC2
Omaha, NE 68183

Attention: Marc Kraft, Mary Ann Borgeson, Clare Duda, Mike Boyle, PJ Morgan,
Chris Rodgers and Pam Tusa

Tom Cavanaugh, Douglas County Clerk/Comptroller
John Ewing, Douglas County Treasurer
1819 Harney St.
Omaha, NE 68183

Dear Commissioners, Mr. Cavanaugh, and Mr. Ewing:

I have completed an audit of Douglas County Oracle user access. The purpose of the audit was to assess the adequacy and effectiveness of the control processes used to ensure that access to Oracle user applications are properly granted and continually assessed. The audit revealed that, overall, controls were adequately designed and worked effectively. However, there were exceptions related to segregation of duties. Details appear in the Findings section below.

Background

As part of the fiscal year audit plan, Douglas County Internal Audit performs internal control testing for the Douglas County external audit firm, Hayes and Associates, LLC. The external auditor uses the test data provided by Internal Audit to formulate a professional opinion about the County's year-end financial statements. Below are the details related to tests of the controls for Oracle user access.

Objectives

The objectives of the audit were to determine that:

- Employee Oracle user access is authorized and approved by appropriate personnel.
- There are appropriate controls in place to ensure that Oracle users' access rights are restricted to the functions that are essential to their job description and that the access does not create a segregation of duty conflict.
- Oracle user access for all employees is periodically assessed for propriety.

Scope and Methodology

The audit included a review of thirty randomly chosen Oracle access requests from July 1, 2011 through June 30, 2012. The sample was chosen using the current and prior active Oracle user listings. The review verified that the access requested was approved by the appropriate managers and that the access granted was the access authorized. Generation of appropriate notices and removal of access was also verified for Oracle users upon termination.

The periodic assessment of user access was reviewed to determine how user access was evaluated. Additionally, the duties of all Douglas County employees with the ability to update data within Oracle were analyzed to determine if there were any segregation of duty conflicts. Lastly, all active users were reviewed to determine that they were active employees based upon a listing provided by Human Resources

Findings

Conflicts of Duties

Criteria: Access to accounting and financial records should only be provided in accordance with management's approval which provides for adequate segregation of duties. Those duties should be periodically assessed and include an evaluation to ensure that current system access provides for adequate segregation of duties and that employees have only the access needed to do their jobs.

Condition: Analysis of Oracle user access revealed exceptions related to employees with incompatible duties and terminations. The exceptions noted follow:

- Four employees had Oracle access that provided the ability to apply receipts to customer invoices and had access to the cash receipts. (This is a repeat finding from the previous audit.)
- Two employees had the ability to enter accounts payable invoices and post batches into Oracle and also had access to returned checks.
- One employee had Alert Manager access and the ability to change various master data files. Alert Manager enables the user to direct who would be alerted when the master data is changed. (This access was removed subsequent to year-end per independent Clerk/Comptroller Office analysis.)
- One employee had access to apply receipts to customer invoices, but did not need the access to perform her job function. (This access was removed subsequent to year-end per independent Clerk/Comptroller Office analysis.)

Effect: The effects of the above conditions are outlined below:

- The employees who had access to apply customer receipts and had access to the receipts had the opportunity to convert receipts to personal use and possibly avoid detection.
- Having the ability to post accounts payable entries and having access to returned checks provided the ability to create improper disbursements that could be converted to personal use and possibly avoid detection.

- Having the ability to change master data and the ability to determine who receives master data changes by using Alert Manager provided the ability to make unauthorized or inappropriate changes to master data and possibly avoid detection.
- A Corrections employee had access to apply receipts but did not use the functionality. Having more access than was needed to do their job violated one of the fundamental rules in granting system access.

Cause: The causes for the applicable items noted above appear below:

- The Treasurer’s office does have a procedure in place to mitigate the risk associated with their employees applying receipts and having access to the receipts.
- The County Clerk/Comptroller returned check policy did not provide for complete segregation of duties.
- Earlier assessments of Oracle user responsibilities did not bring to light that Alert Manger access was inappropriate for the user.
- DotComm personnel used only the access request form and did not regard the email that indicated cash receipting should not be provided.

Recommendation: The following recommendations are made to help address the issues identified above:

- The Treasurer’s Department should Draft County-wide standards outlining the appropriate procedures to follow when receiving and applying cash receipts.
- Ensure that the employees with the ability to apply cash do not have access to the cash receipts or provide mitigating controls to ensure all receipts in their possession is deposited intact.

Management’s Response: The Treasurer’s Office will re-implement the procedure of adding the check items that are mailed to the Accounting Division for processing. The Treasurer’s Office is also exploring the use of the remote capture banking feature for processing checks that are mailed to the Treasurer’s Office Accounting Division.

- Consider immediately voiding returned checks. As an alternative, consider keeping returned checks in the possession of personnel who do not have the ability to post/enter Oracle accounts payables. This person should ensure that checks remained are not changed in any way. In all cases there should be independent assurance that reissued payments have been handled properly including voiding returned checks and ensuring that all master data changes were appropriate and approved by management.

Management’s Response: Management concurs. The Clerk/Comptroller has implemented a policy wherein all returned checks are stamped “void” by Administration staff who open the mail, prior to the current logging and follow up procedures. Also, an additional procedure has been put in place so that an accountant in the Finance Division includes a review of the returned checks and their disposition in the monthly audit of check stock/issuance/re-issuance records.

- Incorporate a more systematic process for reviewing user access requests and periodic access reviews. Remove from the form requests for access that are not needed. Require complete and thorough descriptions of all duties performed outside of Oracle and within Oracle if the access requested includes updates to transactions or master data. Consider creating fields for functions that would conflict with update access. Consider performing access reviews each quarter documenting increased consideration to employees having the ability to create/change transactional or master data.

Management's Response: Quarterly reviews have been performed by Clerk/Comptroller staff (annual was all that was required by prior external auditors) for several years; we will work to better document these reviews. The Oracle access request form has recently undergone major changes; the Clerk/Comptroller's office will work with the City of Omaha to further revise this shared Oracle access request form to attempt to comply with the recommendation. In regards to the Alert Manager responsibility, Clerk/Comptroller employees had to teach DOT.Comm employees how to set up Alerts in Oracle; when this training process was completed, the Clerk/Comptroller's office requested termination of the access.

Audit Standards

Internal Audit conducted this audit in accordance with generally accepted government auditing standards. Those standards require that the audit is planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for its findings and conclusions based on the audit objectives.

Internal Audit has reviewed this information with the Chief Deputy Douglas County Clerk, The Douglas County Treasurer, Chief Deputy Douglas County Treasurer and the Treasurer's Senior Director of Accounting/Auditing. Internal Audit appreciates the excellent cooperation provided by management and staff. If you have any questions or wish to discuss the information presented in this report, please contact Mike Dwornicki at (402) 444-4327.

Sincerely,

Mike Dwornicki
Internal Audit Director

cc: Paul Tomoser
Joni Davis
Trent Demulling
Donald Stephens
Kathleen Kelley

Joe Lorenz
Patrick Bloomingdale
Tim Cavanaugh
Kathleen Hall
Patricia Carter
Mark Rhine