



Douglas County Internal Audit

June 22, 2015

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

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

Thomas F. Cavanaugh, Douglas County Clerk/Comptroller
1819 Harney St.
Omaha, NE 68183

Dear Commissioners and Mr. Cavanaugh:

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 a lack of timeliness in removing the access of terminated users and in detecting inappropriate access of current or terminated users.

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. Oracle is the computer system used to generate financial information for the County. Below are the details related to tests of the controls for Oracle user access.

Objectives

The objectives of the audit were to determine that:

- 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 is periodically assessed to determine that current access is appropriate.

Scope and Methodology

The audit included a judgmentally chosen examination of ten additions and twenty terminations from July 1, 2014 through May 8, 2015. The sample was chosen using the current and prior active Oracle user listings. The additions were tested to verify that the access requested was approved by the appropriate managers and that the access granted was the access authorized. The generation of appropriate termination notices and removal of access was also tested.

The periodic assessment of user access was reviewed to determine how user access was evaluated. Additionally, the duties of all persons with the ability to update data within Oracle were analyzed to determine if there were any segregation of duty conflicts. Mitigating controls where possible segregation of duty conflicts existed were identified and confirmed to be in place and operating as described. Lastly, all active users' employment status was reviewed to determine that users were currently employed by Douglas County or a related entity based upon Human Resources data or confirmation with management.

Findings

Terminations

Criteria: IT user access that is no longer needed should be removed in a timely manner. Removal of access more than seven days after the termination date was considered an exception.

Condition: Twenty employee terminations were tested to see how long it took to remove their Oracle user access. For eleven of the twenty, it took more than seven days after the user had already left employment for system administration to remove their access. In four of the eleven cases, terminations notices from Human Resources were sent after the user had left the County. On average, access was removed eighteen days after the termination date for the twenty terminations tested.

Effect: The users noted above had access that provided them abilities to enter or change limited types of data in Oracle. It is unlikely their access and current status could be used to convert assets to personal use or access sensitive data. However, this may not always be the case if unneeded access is not prevented or detected in a timely manner.

Note: The access of the users noted above was removed prior to issuance of this report.

Cause: The processes currently in place are not adequately designed to provide assurance that the access for terminated employees, non-employee users or users transferring to different job functions would be changed in a timely fashion. DOT.Comm did not have adequate staffing to perform the terminations in a timely manner or a policy in place to require terminations in a reasonable amount of time and a process to measure the amount time to remove access.

Recommendation: Adopt a policy using best practices for terminations. This would require access removal within twenty-four hours. Regularly measure the amount of time it takes to

remove access and actively work to monitor the process for improvements. Educate the County's departments and affiliated agencies on the need to inform the County HR Department when terminations or job transfers occur so that termination notices can be sent out in a timely manner.

Management's Response: DOT.Comm is drafting an official policy on User Terminations for the Oracle E-Business Suite which will be enforced by an automated process.

DOT.Comm is automating the termination of employees within 24 hours of them being terminated in HR in the Oracle E-Business Suite. The process will execute once per day and will remove all access except for Employee/Retiree Self Service which can be used to view personal payroll information and the employee's W-2. Any employee leaving for any reason besides retirement will have their Employee/Retiree Self Service responsibility removed on May 1st of the following year. This allows them to have access to their W-2 through April for income tax filing purposes.

This solution does require a timely termination to be entered in the HR module in order for the process to remove access in an automated fashion. DOTComm should still be contacted immediately to remove access in cases when there is a fear that the terminated individual may attempt to access the system for malicious purposes.

Access Monitoring

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: An examination of all current Oracle users showed that there were six users that were no longer employed by the County or a related entity - four were County employees and two were Juvenile Probation employees. Additionally, there were two Treasurer's office employees that had Oracle AR receipting access while they were doing bank reconciliations. The person who normally prepares bank reconciliations had their Oracle AR receipting responsibility approved using the access form, but did not disclose that their regular duty was performing bank reconciliations.

Effect: The six terminated users noted above had access that provided them abilities to enter or change limited types of data in Oracle. However, it is unlikely their access could have been used to convert assets to personal use or access sensitive data and avoid detection. This may not always be the case if unneeded access is not detected in a timely manner.

It was noted in prior audits that persons who posted cash receipts also had physical access to the receipts. This provides an opportunity to convert assets to personal use and possibly avoid detection. The Treasurer's office had controls in place to mitigate the conflict. Having persons who post cash and reconcile bank accounts as noted in the Condition section above reduces the effectiveness of the mitigating controls.

Note: The Oracle AR Receipting access of the bank reconciler was removed prior to the issuance of this report.

Recommendation: Train all persons filling out Oracle access forms on the necessity of disclosing all duties performed by the persons needing access. Maintain a database of all employees' duties that could cause a conflict with Oracle responsibilities. Require all County offices to periodically provide the duties of their Oracle users. Use the database in the monthly assessment of Oracle users' responsibilities.

Management's Response: Beginning June 1, 2015, all access forms with the job task section not completed are returned to the requesting department for completion. The access request form is being revised to put additional emphasis on all job duties, not just those performed in Oracle. A meeting was held to discuss this process with the Internal Auditor, the Chief Deputy County Clerk, and DOT.Comm Oracle team members. It was agreed that the Chief Deputy would provide a listing to DOT.Comm of Oracle responsibilities that would conflict with other Oracle responsibilities and DOT.Comm would create an automated query that could be run with the monthly review of responsibilities process to identify conflicts impacting appropriate segregation of duties. The Clerk/Comptroller's office will request that this work be completed on or before July 31, 2015. Finally, elected officials and department heads will be required to complete a job task survey for all employees with Oracle access that allows the creation of a record in the financial applications every six months. The responses will be reviewed to assure appropriate segregation of duties.

Audit Standards

Internal Audit conducted this audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. 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 and the IS Manager Oracle. Internal Audit appreciates the excellent cooperation provided by the Clerk/Comptroller's office and DOT.Comm's 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
Jude Lui
Richard File
Patrick Bloomingdale
Joe Lorenz
Diane Carlson
Kathleen Hall
Sheri Larsen
Jerry Prazan
Karen Buche
Tim McNally
Vijay Badal
Frank Hayes
Tumi Oluyole