BERNALILLO COUNTY
NEW MEXICO

SAP Segregation of Duties

Internal Audit

May 2016

REDW LLC
CPAs | Business & Financial Advisors

Bernalillo County Internal Audit
SAP Segregation of Duties

Executive Summary

SUMMARY OF PROCEDURES

REDW performed internal audit procedures over the implementation of the Segregation of Duties module within SAP. Our internal audit focused on testing the process followed by the Enterprise Resource Planning (ERP) team for the identification, evaluation and mitigation of segregation of violations defined within the SAP system. This process included identifying roles with segregation of duties violations, working with the various departments in determining appropriate risk levels for these roles, and mitigating the risks by either removing specific access or assigning manual controls to the departments. REDW further reviewed the access given to the ERP Business Support Analysts, the process for adding and removing access within the SAP system, and the assignment of risk as understood by each department.

We performed the following procedures:

- Obtained an understanding of the process followed by ERP for identifying, analyzing and mitigation of SAP segregation of duties violations through interviews with ERP personnel and inspection of relevant documentation.
- Obtained a listing of roles that were identified as segregation of duties risks, and tested a sample to determine the role was evaluated, an appropriate risk level was assigned, and the SAP system had been properly updated to reflect the analysis.
- Evaluated a sample of ERP Business Support Analyst roles to determine the access granted had been reviewed and appeared appropriate for the department(s) that the Business Support Analyst supported.
- Obtained a listing of new users and transfers from the SAP system for fiscal year 2016 to evaluate the roles granted were approved, assigned or inactivated appropriately, timely, and that all supporting documentation was on file.
- Obtained a listing of departments that ERP had worked with on the evaluation and mitigation of segregation of duties risk as of May 2016 to determine the risk levels and mitigating controls were properly assigned, and controls were properly functioning. Additionally, we inquired with the departments about the monitoring process that should take place as the segregation of duties monitoring processes continue to be developed.

SUMMARY OF OBSERVATIONS AND RECOMMENDATIONS

REDW observed areas during the course of the audit where controls were functioning properly and established procedures were followed. Most notably was the change and improvements that the ERP team made in identifying the segregation of duties conflicts and the improvements made towards completing the mitigation process.

As a result of our testing, the following significant high and moderate risk observations were identified:

- **Risks Identified Did Not Follow Action Plan –** Critical and High risk SOD violations which were identified by ERP for mitigation did not follow the action plan discussed with the user departments and did not have documentation of the current status readily available.
- **Inappropriate Access for Support Roles –** Business Support Analysts have access to update and modify areas within SAP that are not relevant to their daily job responsibilities. This access is not reviewed or monitored to ensure inappropriate changes or transactions are not being made.
- **Monitoring Responsibilities not Identified –** County departments have not identified or implemented internal controls around the risks identified in SOD mitigation. ERP and County departments have not made a clear determination of who is responsible for SOD risk mitigation.
- **User Access Reviews not Performed –** There is no process in place for department management to review their department's users within the SAP system to determine the appropriate individuals have access to perform their job responsibilities.

* * * * *

Further detail of our purpose, objectives, scope, and procedures are included in the internal audit report.

We received excellent cooperation and assistance from the ERP team during the course of our interviews and testing. We sincerely appreciate the courtesy extended to our personnel.

REDW LLC

Albuquerque, New Mexico
July 25, 2016

Bernalillo County Internal Audit
SAP Segregation of Duties

Table of Contents

REDW LLC
CPAs | Business & Financial Advisors

redw.com

Bernalillo County Internal Audit
SAP Segregation of Duties

Report

INTRODUCTION

We performed the internal audit services described below solely to assist Bernalillo County in evaluating selected processes relating to SAP Segregation of Duties identification, analysis, and implementation. Our services were conducted in accordance with the Consulting Standards issued by the American Institute of Certified Public Accountants, Generally Accepted Government Auditing Standards, and the terms of our contract agreement for internal audit services. Since our procedures were applied to samples of transactions and processes, it is possible that significant issues related to the areas tested may not have been identified.

An entrance conference was held on April 18, 2016, and fieldwork began the week of May 23, 2016. An exit conference was held on June 20, 2016.

PURPOSE AND OBJECTIVES

During the 2011 internal audit over SAP User Access Controls, there were segregation of duties risks identified in SAP. From this audit, a recommendation was made that ERP implement a plan to put into place mitigating controls over identified segregation of duties risks. We were informed that the segregation of duties mitigation has been in process for approximately 5 years and that ERP team members responsible for updating the roles have changed over time. Therefore, our internal audit focused on assessing the process ERP followed when identifying, analyzing and mitigating segregation of duties issues within SAP at the role level. We reviewed the processes related to: individual role segregation of duties mitigation, ERP Business Support Analyst access, and the processes followed for new hires and terminations. Additionally, we inquired with departments in which the ERP team had worked to determine risk levels for their respective roles, the process for identifying mitigating procedures, and the continual process for monitoring known segregation of duty risks.

SCOPE AND PROCEDURES PERFORMED

In order to gain an understanding of the processes and operations, we interviewed the following personnel:

- Randy Landavazo, ERP Manager
- Juan Flores, IT Supervising Analyst (Technical)
- Joseph Neeham, IT Supervising Analyst (Functional)
- Bang Hang, IT Administrator
- Robert Benevidez, CIO
- Rod Rolston, Deputy CIO
- Elie Boujaoude, Deputy CIO
- Jackie Sanchez, Financial Administrator
- Anthony Infantino, Financial Projects Coordinator
- Cindy Torres, Accounting Officer

In order to understand the process followed we read relevant portions of:

- The GRC Access Control 10.0 Blueprint

We performed the following testwork:

Segregation of Duties Process at the Role Level: Obtained a listing of all SAP roles that had been evaluated for segregation of duties conflicts as of May 2016 and selected 25 (of 39 total) focusing on roles with high and critical risk levels. We tested to determine:

- Roles were evaluated and assignments of risk levels were documented.
- ERP team followed the action plan developed based on the risk analysis completed.
- Roles within the SAP system were properly updated to reflect the changes as defined by the action plan. Additionally, critical risks were mitigated in the SAP system and high risks were mitigated through manual controls.

ERP Business Support Analyst Roles: Obtained a listing of all Business Support Analysts with functional SAP roles as of May 2016 and selected a sample of 3 (of 19 total) to determine what actions were taken to mitigate conflicts. We tested to determine:

- Access granted was appropriate through discussions with management and supporting documentation.
- Access to back-up support roles was appropriate and a process was in place to monitor back up duties performed.

New Hire and Termination Processes: Obtained a listing of all new hires and terminations within SAP for fiscal year 2016 and selected a sample of 6 new hires and 4 terminations. We tested to determine that the:

- Roles were assigned/removed properly.
- Process was completed timely.

- Supporting documentation and approvals were appropriate and maintained.
- Requests were appropriately reflected within the SAP system.

ERP and Department Communication: Obtained a listing of module areas that the ERP team had worked with in assigning appropriate role risk levels. REDW selected 3 (of 6 total) to discuss the segregation of duties process and gain an understanding of the department's activities related to the project. REDW inquired with the departments regarding the assignment of critical and high risk roles, their understanding of the mitigation procedures, and any follow-up procedures necessary to complete role level implementation. Additionally, we discussed, with selected module owners, the need for ongoing monitoring of segregation of duty issues, and through these discussions worked to identify where the ERP department and the module owners can improve ownership of future monitoring procedures.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

As a result of our testing, REDW identified the following observations:

1) Risks Identified Did Not Follow Action Plan

Critical and High risks within SAP were evaluated and mitigated by ERP. Based on this evaluation, an action plan was created to update the roles and assign manual mitigating controls to address the identified risks. While all roles selected for testing had been evaluated by the ERP team, our testing determined 18 of 25 roles had not completed the action plan defined by ERP. Roles marked for updates remained unchanged in the system and documentation over the current status of each role was not readily available.

- Twelve of the 25 roles tested were listed as critical risk roles by ERP that should have an offending T-code removed; however, as of May 2016 the offending T-code was still tied to the role and flagged as critical within the system.
- Six of 25 roles tested did not match what was listed in the ERP action plan and there was no readily available supporting documentation to validate the changes that occurred.

Our testing further determined that there was no comprehensive process in place to monitor the mitigation status of each role. There was no defined timeline for completion of this process, and ERP team members who were responsible for the implementation did not have dedicated time to focus on the project.

Potential Risk: High – Due to the volume of roles that are in the mitigation process without a tracking mechanism and a timeline for completion, risks are left unmitigated or never fully complete the role mitigation process.

Recommendation: The County should determine a formal plan and tracking process for the completion of the SAP risk mitigation. The plan should include dedicating specific ERP team members to make the SAP clean-up process a priority, and include a timeline for completion. Formal documentation and monitoring of this plan will help to ensure continuity of information between members of ERP and User Departments.

Management Response: ERP is developing a formal plan to redesign system roles and tracking of risk mitigation processes. We are working with our consulting company to develop a clearly defined timeline for completion. This timeline will be critical in the implementation and completion of GRC initiative, so constant monitoring of progress will be imperative. Additionally, we agree that our team, once assembled, should be consistent throughout the process, as changes to the team may cause undesired repercussions to the implementation and timeline of the GRC endeavor. Completion of the GRC tasks, shown below, are expected to occur by December 31, 2017.

GRC Task Names
Develop Request for Response (RFR)
Vendor Response to RFR
Validate Business Processes
Project Preparation and Requirements Gathering Phase
Role Change Management
Roles Analysis & Design
Role Redesign Phase
Role Building Phase
Role Testing Phase
Access Risk Analysis Phase
Final Preparation Phase
Go Live Phase
GRC Post Go Live Validation and Stabilization

2) Inappropriate Access for Support Roles

The ERP Business Support Analysts provide support to various departments throughout the County. Business Support Analysts are granted full access to each of the departments that they directly support as well as any department for which they perform back-up duties. There was no review process in place to ensure that the access granted to the Business Support Analysts was appropriate. All three Business Support Analyst roles tested did not have appropriate access for the job responsibilities and back-up duties assigned.

Potential Risk: High – The access granted to Business Support Analysts allows them to make changes within SAP without a monitoring process in place to verify the changes are appropriate. This access creates a heightened risk of inappropriate transactions and unauthorized changes being made within the SAP system.

Recommendation: The County should implement a periodic review process over Business Support Analyst support roles to determine what access is appropriate and necessary to complete their support functions.

Management Response: We will be removing Business Support Analyst support roles that allow for making changes to Production and replacing with a new process for our support personnel to assist our customers. ERP management is creating a plan that includes utilizing remote control viewing software to assist users accomplish tasks within the SAP application. By remotely viewing into a user's system, with their explicit consent, ERP personnel can help them accomplish their tasks by guiding then to make the appropriate actions to their system environment. This allows us to support our users without ERP staff requiring support role access inconsistent of their primary duties. This will be put into action by December 31, 2016.

3) Monitoring Responsibilities not Identified

The ERP team worked to update roles within the SAP system to allow users to perform business functions even though they have conflicting SOD violations. ERP worked with the County departments to determine what action should be taken for each role flagged with SOD violations. Once ERP had updated the roles as discussed, the departments are responsible for monitoring the created SOD risks through manual controls. As of testing in May 2016, the departments were not performing monitoring controls and there was confusion over where the responsibility was for the continued monitoring of the SOD risks.

Potential Risk: High – SOD risks within SAP, which are not monitored through system mitigation (ERP) or manual mitigating controls (Department level), create a heightened risk that an unauthorized transaction would be performed without being caught.

Recommendation: ERP should determine an appropriate process for ensuring the SAP system is secure and that risks identified within the SAP are effectively mitigated. County Departments should be responsible for implementing internal controls for their business processes to ensure there are no SOD violations. County management should work with departments to implement internal controls (or mitigating controls) and procedures to ensure that monitoring for SOD risks within SAP occur.

Management Response: The finding is to be handled the same as Audit Finding #1: ERP is developing a formal plan to redesign system roles and tracking of risk mitigation processes. We are working with our consulting company to develop a clearly defined timeline for completion. This timeline will be critical in the implementation and completion of GRC initiative, so constant monitoring of progress will be imperative. Additionally, we agree that our team, once assembled, should be consistent throughout the process, as changes to the team may cause undesired repercussions to the implementation and timeline of the GRC endeavor. Completion of the GRC tasks, shown below, are expected to occur by December 31, 2017.

GRC Task Names
Develop Request for Response (RFR)
Vendor Response to RFR
Validate Business Processes
Project Preparation and Requirements Gathering Phase
Role Change Management
Roles Analysis & Design
Role Redesign Phase
Role Building Phase
Role Testing Phase
Access Risk Analysis Phase
Final Preparation Phase
Go Live Phase
GRC Post Go Live Validation and Stabilization

4) User Access Reviews not Performed

Users are granted access to SAP to perform daily job responsibilities. As job responsibilities change due to promotions, transfers, or terminations, so does their access within SAP. There is a form available for departments to fill out and send to ERP to update the access accordingly. Although there is a process in place for making sure the change was appropriate, there are currently no review procedures performed at the department level to determine users within their group have appropriate access.

Potential Risk: Moderate – A user with inappropriate access could have the ability to perform unauthorized transactions within SAP.

Recommendation: On an annual basis, department level managers should be reviewing their employees' access to SAP to determine if the access is still appropriate and necessary for job responsibilities. ERP can generate an access report and help to facilitate the annual review by departments.

Management Response: This finding will be addressed in two different phases. First, ERP will generate a biannual report detailing the user access for departments, which will be sent to department directors. Departments will then be responsible for reviewing and supplying changes to access to ensure that employees' user access is still appropriate for their job responsibilities. The first report will be generated by December 31, 2016.

Upon completion of GRC role redesign initiative, we will utilize a more automated process. In phase 2, we will utilize the GRC automated reporting to ensure that role assignments to end users are consistently reviewed and approved periodically, at least every six months. Departments will then be responsible for review and supplying changes to access.

5) Terminated Users Not Removed Timely

Users who are terminated or who transfer roles within County are communicated by Human Resources (HR) to the ERP team on a weekly basis. ERP is responsible for working with the department in removing the users' access timely. REDW identified 1 of 4 terminations where the inactivation process took 24 days to complete.

Potential Risk: Low – If a terminated user's access is not inactivated in a timely manner, the employee could potentially have unauthorized access to the SAP system. REDW categorizes this risk as low due to additional controls in place, such as restricted access to the building and computer hardware after termination.

Recommendation: The County should work to ensure the process to remove users' access to SAP is completed as soon as the employee is terminated. The ERP team should respond to the HR emails as quickly as possible to mitigate the risk of a terminated user having unauthorized access to the SAP system.

Management Response: The employee status dissemination process has been streamlined with HR for ERP to receive county employee status updates on a daily basis. This has allowed ERP to update our system in a substantially quicker manner than was possible when we were receiving updates on a monthly basis. ERP now receives notifications and takes same-day action to make the appropriate updates within the SAP system.

* * * * *

This report is intended for the information and use of Bernalillo County management, the audit committee, members of the Board of Commissioners of Bernalillo County and others within the organization. However, this report is a matter of public record, and once accepted its distribution is not limited.

We discussed and resolved minor observations with management and received excellent cooperation and assistance from ERP during the course of our interviews and testing. We sincerely appreciate the courtesy extended to our personnel.

REDW LLC

Albuquerque, New Mexico
July 25, 2016