SAP Segregation of Duties

Internal Audit

February 2018

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 SAP system. Our internal audit focused on evaluating selected controls and processes related to users' roles, segregation of duties violations, IT Analyst-Business System Analysts (IT-BSA) access, and user access reviews. Additionally, we performed procedures to determine if observations from the May 2016 internal audit report were addressed.

We performed the following procedures:

- Obtained an understanding of the status of the segregation of duties project to mitigate critical/high segregation of duties conflicts within SAP roles.
- Obtained a listing of users with critical/high risks that had not been updated as of February 28, 2018, and compared the listing to total SAP users and users updated in January 2018 to determine the status of the SAP role updates project.
- Obtained an understanding of the process for utilizing firefighter identifications (IDs) to perform conflicting duties. Selected a sample of actions completed using the firefighter ID and tested to determine if the user was approved to use the firefighter ID, the actions were documented and matched the action performed, the activity was reviewed by the IT-BSA owner and the activity was reviewed timely.
- Selected a sample of new users added to the SAP system after the implementation of the Governance Risk and Compliance (GRC), and tested to determine if the request was appropriately approved, the users did not have critical/high risks associated with their role, and the roles that were requested agreed to the roles assigned.
- Requested a sample of bi-annual user access reviews to determine if the reviews were performed, and all departments responded to the requests. We were unable to test this process as no user access reports had been completed.
- Obtained the most recent bi-annual inactive user review, which evaluated users who had been inactive for 180 days, and tested to determine if the report was provided to respective department, and any changes communicated by the department to Enterprise Resource Planning (ERP) were completed.

Albuquerque
7425 Jefferson St NE
Albuquerque, NM 87109
P 505.998.3200
F 505.998.3333

Phoenix
5353 N 16th St, Suite 200
Phoenix, AZ 85016
P 602.730.3600
F 602.730.3699

- Obtained a listing of all IT-BSAs, including all functional roles within SAP. Selected a sample of IT-BSA roles, and tested to determine if the access granted had been reviewed and appeared to be appropriate for the departments that the IT-BSA supports.

Summary of Observations and Recommendations

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

1 ***GRC Implementation:*** As of February 28, 2018, ERP has only evaluated approximately 76% of users having high and critical risks. We recommend ERP complete the evaluation of all users with critical and high risks as soon as possible.

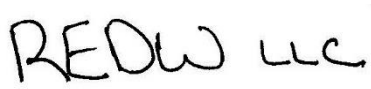
2) ***Firefighter Actions:*** In evaluating a selection of transactions performed using firefighter IDs, we identified 16 sessions having variances between the actions the user requested to perform and the actual transaction performed, 13 sessions that had not been reviewed and 18 sessions whose review was performed over 10 days after firefighter ID was checked in. As such, performance measures should be established to ensure completion of timely reviews through evaluation of role distributions and assigning of backups.

3) ***Firefighter IDs:*** Twelve firefighter IDs had not been properly set-up causing actions performed using those firefighter IDs to not be sent for review to the pertinent IT-BSA. Going forward all new firefighter IDs should be reviewed to ensure they are properly set up to track activity and send notifications to the appropriate IT-BSA for review.

4) ***Overreliance on Consultant:*** The ERP department relies heavily on a Consultant in navigating through SAP, answering questions and running reports. Training should be obtained for all employees to ensure the ERP can perform key tasks without immediate assistance from the Consultant.

* * * * *

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



Albuquerque, New Mexico
April 10, 2018

Bernalillo County Internal Audit
SAP Segregation of Duties

Table of Contents

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 controls and processes relating to the implementation and monitoring of segregation of duties within the SAP system. 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 February 23, 2018, and fieldwork began the week of February 26, 2018. An exit conference was held on April 2, 2018.

PURPOSE AND OBJECTIVES

The SAP system is an enterprise resource planning software which incorporates key operational functions at Bernalillo County. As part of a follow-up to an internal audit from May 2016, we evaluated the status of the recently implemented Governance Risk and Compliance (GRC) implementation process. GRC was implemented in order to mitigate conflicting actions performed by SAP users. As part of the GRC implementation process, certain users were assigned firefighter IDs, which allow them to perform conflicting actions. All actions performed under a firefighter are then reviewed and approved by an IT Analyst-Business System Analyst (IT-BSA).

Our internal audit focused on selected controls and processes over the implementation and monitoring of segregation of duties within the SAP system. We reviewed the processes related to individual role segregation of duties mitigation, firefighter ID access, new hire access and IT-BSA access. Additionally, we performed procedures to ensure that observations from previous audit reports were being addressed.

Albuquerque
7425 Jefferson St NE
Albuquerque, NM 87109
P 505.998.3200
F 505.998.3333

Phoenix
5353 N 16th St, Suite 200
Phoenix, AZ 85016
P 602.730.3600
F 602.730.3699

SCOPE AND PROCEDURES PERFORMED

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

- Joseph Needham, ERP Functional Manager
- Juan Flores, ERP Technical Manager
- Bang Hang, SAP Security Administrator
- Michelle Bates, IT Administrator
- Jagadish Sudhakar, Consultant
- Edwina Zamora, Business System Analyst
- Tanya Komogorova, Business System Analyst
- Donny Daniels, Business System Analyst

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

- Firefighter- Quick Reference Guide
- Firefighter ID Controller- Quick Reference Guide
- Firefighter ID Owner- Quick Reference Guide
- Access Control Team- Quick Reference Guide
- Role Owner- Quick Reference Guide

We performed the following testwork:

GRC Implementation: Obtained an understanding of the GRC implementation process for identifying, analyzing, and mitigating SAP segregation of duties violations. Obtained a report from the SAP system as of February 28, 2017, listing of all users with critical/high conflicts who had not been updated to remove segregation of duties conflicts in order to determine the completion progress.

Firefighter Actions: Obtained listing of all actions completed using a firefighter ID since implementation (December 7, 2017 to February 20, 2018). We selected a sample of 40 of 222 actions completed using the firefighter ID, and tested to determine if:

- The user was approved to use the firefighter ID.
- The user documented the reason for using the firefighter ID and the completed actions matched the reason.
- The firefighter activity was reviewed by the IT-BSA.
- The IT-BSA reviewed the action timely.

New Users: Obtained a listing of new users added to the SAP system from implementation through fieldwork (December 19, 2017 to February 15, 2018). We selected a sample of five users from a total of 14, and tested to determine if:

- Proper approval was received to provide the user access.
- User was not granted a role with critical/high segregation of duties risks.
- Roles requested agreed to the roles assigned.

User Access Review: Requested the two most recent bi-annual user access reports to determine if:

- The User Access Review was provided to departments.
- The department responded timely with any updates to user access and ERP made the relevant changes.

Inactive User Review: Obtained the inactive user review performed in December 2017, which evaluated users who had been inactive for over 180 days, and tested to determine if:

- The report was provided to respective departments.
- Departments provided a response to ERP.
- Any changes communicated by the departments were completed.

IT Analyst-Business System Analysts Role Evaluation: Obtained the listing of all IT-BSAs, including all functional roles within SAP, as of February 20, 2018. We selected a sample of three IT-BSAs from a total of nine, and tested to determine if their access agreed to the designated modules listing, and the access appeared to be appropriate based on the department that the IT-BSA supported.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

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

1) GRC Implementation

During the prior audit in May 2016, it was identified that users with critical/high risks had not been evaluated or mitigating actions implemented. According to Management's response, GRC implementation was expected to be completed by December 31, 2017. As of February 28, 2018, there were 113 users (approximately 24% of total users with critical/high risks) that had not been evaluated and mitigated. These users had critical/high risks associated with their SAP role, and there were no monitoring procedures performed to determine if the user's actions were appropriate.

Potential Risk: ***High*** **–** As GRC has not been fully implemented to update all users, there continues to be a large amount of users whose actions are not being monitored. This can result in users potentially performing erroneous transactions or transactions outside of their duties without the possibility of someone detecting them.

Recommendation: ERP should complete the evaluation of all users with critical/high risks as soon as possible.

Management Response: Currently, we are at 80% complete for removing roles and moving to firefighter account access for remaining users not already complete for Segregation of Duty. We expect to be at 90% by June 30, 2018, as we have upcoming End of Fiscal year activity that will be taking priority until July 1, 2018. We expect to be at 100% by September 30, 2018. This date will then allow us to finish the system component that will track user access review processes.

2) Firefighter Actions

As part of the GRC implementation, users with critical/high segregation of duties conflicts in SAP are assigned firefighter IDs to perform the conflicting duties. Any actions performed using the firefighter ID are tracked and must be reviewed by a IT-BSA to determine if the actions performed were appropriate. We selected 40 actions, which were each part of a firefighter ID session and identified:

- Sixteen sessions had variances between the documented action and the actual action performed.
- Thirteen sessions were not reviewed by the IT-BSA as of testing, ranging between 8 and 30 days.
- Eighteen sessions had the review performed over 10 days after firefighter ID was checked in.

Potential Risk: *High* – The purpose of assigning firefighter IDs was to ensure conflicting actions are monitored and reviewed. If there is a large lag time between the completion of an action and the review, there is a risk that an unauthorized transaction may not be caught timely. Additionally, as the firefighter ID allows the users to perform conflicting tasks, users should have a valid reason to use the firefighter ID. If the user does not document the reason for utilizing the firefighter ID in accordance with the procedures, there may be a risk that IT-BSAs do not review all the transactions performed.

Recommendation: Performance measures should be established to ensure IT-BSAs complete reviews timely. If needed, ERP should evaluate the IT-BSA role distribution and assign backups to assist any IT-BSAs with a higher number of reviews to perform. Additionally, ERP should educate users with firefighter ID access and explain the importance of properly documenting all actions performed, and encourage the use of additional comments prior to ending a session.

Management Response: We will review our process for reviewing firefighter logs to determine an appropriate sampling level of reviewable-logged items and an appropriate timeframe in which to accomplish the review. The suggestion of 10 days may be appropriate, but we need to review that suggestion based on our amount of logged items, sampling rate, and resource availability. We expect to have our process review done to determine sampling rate and review timeframes, and have those determined values established and in place, by the end of December 2018.

At the initial deployment of the new GRC system, the process to add additional activity notes was unclear to some of the reviewers, which precluded them from documenting their additional activity performed. This training oversight has since been corrected and we are working with our users to ensure they understand the process to correctly add documentation for additional activity. It is important to note that there will still be transactions that will be logged, by way of the system using other transactions, which are transparent to the person who checked out the account and therefore cannot be added as an additional activity. Therefore, there will be instances where there will be transactions recorded that will not be in the “expected action to be performed” nor the “additional activity” areas. However, these transactions are still in the log of transactions performed and, as such, are still part of the review process.

3) Firefighter IDs

After a user has completed a session using a firefighter ID, the IT-BSA (controller) will receive a notification from the systems workflow indicating that a new work item is ready for review and approval. As we obtained an understanding of the review process, it was identified that 12 firefighter IDs had not been properly set up, causing them to not be sent to the IT-BSA for review.

Potential Risk: *High* – If the system is not properly set up, unauthorized activity could occur and go undetected.

Recommendation: Although we verified there were no other firefighter ID's being excluded from the workflow notification, we suggest going forward for all firefighter IDs be reviewed in order to ensure that they are properly set up to track activity and send the information to the appropriate IT-BSA for review.

Management Response: We will implement a process in which a different security person, other than the one who created the account, will review accounts created, thereby, creating a QA process to help limit the risk of an account not being properly set up. This process is expected to be in place by the end of June 2018.

4) Overreliance on Consultant

In requesting reports and performing inquiries with the Security Administrators and the ERP Technical Manager, it became evident that the department relies heavily on help from the Consultant in order to determine what reports to run and how. During our testing, there were various occasions when we had to contact the Consultant to obtain answers and make basic requests.

Potential Risk: *Moderate* – Instances may arise where the Consultant is not available, and if employees do not have the necessary knowledge to complete a task, there may be a disruption in business functions.

Recommendation: Training should be obtained for all employees with responsibilities related to the GRC implementation and SAP to ensure that the County can perform key tasks without the assistance of the Consultant. Processes should be formally documented as this knowledge is transferred to the ERP team.

Management Response: Knowledge transfer and training opportunities are already underway to help ensure that our employees are obtaining the knowledge to handle as many requests in-house as possible.

5) User Access Review

According to the prior audit report, ERP was to complete a bi-annual access review for all SAP users. A detailed listing of users for each department was to be sent to the departments to confirm the access was appropriate. Departments should approve the access for each individual or request changes, and the ERP team would be responsible for making those updates. No user access reviews were performed in 2017.

Potential Risk: ***Low*** – Currently ERP receives notification of new hires, transfers and termination via emails generated from the Empath system as a mitigating control. However, if an overall user access review is not performed for all SAP users, there is a potential risk that users who have transferred jobs or departments continue to have access to perform old responsibilities.

Recommendation: User access reviews should be performed, at least annually, to review all SAP users' access and ensure that their roles agree to their current job responsibilities. ERP should ensure that all departments respond to the inquiry, and determine if access is appropriate or if changes need to be made.

Management Response: We currently have a mitigating control in place that limits this risk. We receive notices from the Empath HR system that notifies us of personnel moving organization codes. Once received, these users are reevaluated for their access to roles and appropriate changes are made. However, when we have completed the review of remaining users that still have roles in conflict, then the SAP system component that handles this process will be put into place within the GRC application server. As we expect the process of removing roles from those remaining users with roles in conflict to be finished by the end of September 2018, this system implementation is expected to be completed by the end of December 2018.

6) New Users

After the implementation of GRC, all new users are evaluated to ensure their access does not have a critical/high segregation of duties risk, and are assigned a firefighter ID, if necessary. We identified one of five users tested that had been assigned a role with critical/high risks and no firefighter ID was assigned.

Potential Risk: ***Low*** **–** As new users are added and their conflicts are not addressed, they become part of the listing of users who have not been evaluated and are not monitored. If the user is not monitored there is no way to determine if the actions they are performing are appropriate.

Recommendation: The process to add new users should be evaluated to ensure that the roles are assessed for critical/high risk, and if one is identified, the user is to be assigned a firefighter ID. As multiple roles are still under review and modification, with the possibility of the risk level being dropped from high/critical to moderate or low, we encourage such review to be completed as soon as possible. Determining the correct risk level for all roles will help ensure proper mitigation of conflicts by assigned a firefighter ID if necessary.

Management Response: Currently, when we have a new user requesting roles, they are reviewed for critical and high-risk conflicts and assigned firefighter accounts. We will review that process to ensure that we avoid entering users into the system with conflicting roles. Processes identified is expected to be put into place by the end of June 2018.

7) Inactive User Review

Bi-annual inactive user reviews were performed by requesting departments to validate users that had been inactive for over 180 days. For the December 2017 bi-annual inactive user review, there were four of 10 inactive users tested that did not have a department's response after two months.

Potential Risk: ***Low*** **–** There is a potential risk that users who are no longer active could inappropriately obtain access to the system, which could lead to unauthorized use.

Recommendation: A process should be implemented to follow up with departments where a response wasn't received. Alternatively, ERP could establish a deadline date by which department must respond by to avoid inactive users being removed. If no response is received for that department, those users will be deactivated until further notice.

Management Response: We will implement a process to follow up with departments when they have not responded to inactive user queries. If we haven't received a response from a department after two weeks of sending them the request whether an account should be deactivated or not, we will send one final notice letting the department know that the account will be deactivated if a response is not obtained in three business days. We expect this process to be established by the end of June 2018, so that it is in place for our next bi-annual review in July.

PROCESS IMPROVEMENT OPPORTUNITIES

As a result of our testing, REDW identified the following best practice process improvement opportunities:

1) Firefighter ID Session Timeout

Users of firefighter IDs had unlimited time to login and use each ID. The system should give users a limited amount of time to complete tasks in order to ensure other users have the ability to also perform their duties. Most tasks should be able to be completed within an hour.

2) Firefighter Sessions with no Activity

During our testing we noticed multiple firefighter sessions having no actions performed. ERP should communicate to the users that in these situations information should be included on the additional notes section that no actions were completed during use of firefighter ID. Additionally, the system could potentially be set up to not send no activity sessions to be reviewed.

3) IT-BSA Workload

During our interviews with multiple IT-BSA, it was brought to our attention that one IT-BSA in particular is the owner of a large number of firefighter IDs. This causes a delay in the review process as they have more to review. We recommend the workload between IT-BSA to be spread-out in order to ensure a more timely and accurate review.

FOLLOW-UP ON PRIOR-YEAR OBSERVATIONS

Follow-up testing was performed on observation noted during the May 2016 SAP Segregation of Duties internal audit. The status of each observation below was determined through inquiry, testing and/or observation.

Prior Observation 1 – 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.

Current Status: *Unresolved* – See observation #1 above.

Management Response: See observation #1 above.

Prior Observation 2 – *IT-BSA* 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.

Current Status: *Resolved*

Based on testwork performed over IT-BSA role evaluations, it appears access is appropriate based on the department that each IT-BSA supports.

Prior Observation 3- 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.

Current Status: *Unresolved* – See observation #2 above.

Management Response: See observation #2 above.

Prior Observation 4 – 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.

Current Status: *Unresolved* – See observation #5 above.

Management Response: See observation #5 above.

Prior Observation 5 – ERP is responsible for working with the department in removing the users' access timely, however REDW identified terminations where the inactivation process took 24 days to complete.

Current Status: *Unresolved* – See observation #7 above.

Management Response: See observation #7 above.

* * * * *

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.

REDW LLC

Albuquerque, New Mexico
April 10, 2018