REDW LLC

The Rogoff Firm

CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS & FINANCIAL ADVISORS

Internal Audit

SAP User Access Controls

May 2011

Bernalillo County Internal Audit
SAP User Access Controls

Executive Summary

Summary of Procedures

REDW performed an internal audit of the Bernalillo County SAP user access controls. Our consulting services were for the purpose of providing suggestions and recommendations to management to improve the efficiency, effectiveness, and security of the overall SAP user access controls.

In order to determine whether policies and procedures were followed and if adequate controls were in place over SAP user access controls, we performed the following:

- Read the draft business blueprint for SAP implementation dated November 2007,
- Interviewed relevant department personnel,
- Performed walkthroughs of certain critical functions,
- Determined whether access logs were monitored appropriately,
- Evaluated logical user access for selected accounting functions based on job descriptions.

Summary of Observations

We noted the following high or medium risk observations:

- **Lack of current approved access monitoring policies and procedures**—User activity was not regularly monitored to prevent or detect unauthorized access. Policies and procedures should be approved for how often user access logs will be monitored.
- **Untimely employment status notification**—There was a significant time lag between when employees were transferred or terminated by Human Resources and access updated in SAP. This issue is compounded by not having a direct link between the user name and employee identification number. Consultants were not monitored to ensure their access was restricted. Monthly, the ERP Manager should obtain reports from HR that identify the new employees for potential SAP access and the employee transfers or terminations affect SAP access.

- **Incompatible roles existed and built-in SAP modules not utilized**—Users were granted roles not specifically related to their job titles and users had incompatible roles assigned. SAP has built-in functionality to monitor user access, create roles based on job descriptions, and perform audit functions. These modules were either not set up initially or were not working properly. User roles should be set up based on the job description, rather than mirroring existing users, and formal documentation should be created describing which roles should be segregated.

* * * * *

Further detail of our purpose, objectives, scope, procedures, observations, and recommendations is included in the internal audit report. In that report, management describes the corrective action being taken for each observation.

REDW LLC

July 15, 2011

Bernalillo County Internal Audit
SAP User Access Controls

Table of Contents

REDW LLC
The Rogoff Firm
CERTIFIED PUBLIC ACCOUNTANTS | BUSINESS & FINANCIAL ADVISORS

Bernalillo County Internal Audit
SAP User Access Controls

Report

INTRODUCTION

We performed the internal audit services described below solely to assist Bernalillo County in evaluating the processes and procedures over the SAP user access controls. 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.

Although we have included management's responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

PURPOSE AND OBJECTIVES

For this audit, the modules selected were Accounts Payable, General Ledger, Cash Management, and Basis and the department selected was information technology. Our internal audit focused on evaluating policies and procedures over SAP user access controls and establishing whether controls were adequate to actively monitor SAP access in the selected modules and department.

SCOPE AND PROCEDURES PERFORMED

Interviews

In order to gain an understanding of the processes and controls over SAP user access, we interviewed the following personnel:

- Randy Landavazo, ERP Manager
- Andi Lako, Functional Manager
- Dan Stringham, Technical Manager
- Carolina Fernandez, Production Control Analyst/Security

- Bang Hang, Systems Analyst/Security Administrator
- Melissa Maldonado, Business Systems Analyst, Accounts Payable

Background and Understanding

In order to understand ERP responsibilities related to SAP user access:

- We read draft Business Blueprint documents dated November 2007 and other documents provided by ERP.
- We performed process walkthroughs of specific areas covered by this internal audit.
- We read various sections of the book, "Security, Audit and Control Features, SAP R/3, 2nd Edition" published by ISACA.

Testwork

We performed the following testwork:

- Compared the fiscal year 2011 Human Resources (HR) employee listing to the SAP user access matrix and judgmentally selected 56 SAP users to determine if their access to SAP was appropriate.
- Randomly selected 25 SAP users from the SAP user access matrix and tested that their role was properly classified in the system and that they were current Bernalillo County employees or consultants.
- To determine if SAP access was properly segregated within ERP, we selected a sample of 25 SAP users from the Accounts Payable, General Ledger, Cash Management, and Basis modules and evaluated the SAP user roles for processor, approver, and department director segregation.
- Performed a walkthrough of the Accounts Payable department to determine if the department was using the SAP module as designed.
- Performed a walkthrough of one new user's assignment process to determine if validation procedures were performed over that role assignment and were consistent with the business process approach and overall business structure.
- Tested that all SAP user passwords from the SAP user logon report dated May 11, 2011 were changed in accordance with Bernalillo County policies.
- Observed that all SAP default user accounts or profiles had been updated and that the password was not trivial.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

We identified the following weaknesses relating to the Bernalillo County SAP user access controls function.

1) Lack of current approved access monitoring policies and procedures

Although several draft blueprint reports were provided, there were no current written policies or procedures to ensure that ERP staff was properly monitoring SAP user access roles, including the SAP super user accounts. Also, there were no documented procedures for preventing incompatible user duties, ensuring users have proper segregation of duties when roles are created or changed, and monitoring users and those creating user roles.

Recommendation

Written policies and procedures will enable ERP staff to operate more effectively by ensuring routine role creation and monitoring and by facilitating knowledge transfer within the department to reduce the impact of employee turnover. Current processes should be documented in writing and a formal policy should be submitted by the ERP Manager to the CIO. Documentation should include the proper segregation of roles within SAP, the timely monitoring of user accounts, the timely update of employment status, and a requirement to change login passwords at least every 90 days.

Management Response

Although policies and procedures are currently in the development stage, ERP will adopt an existing SAP Application Security Strategy that details SAP best practices in relation to audits and security controls. Furthermore, all internal methodologies, written procedures, notes and processes will be developed and incorporated into the Strategy to include password change-management at the recommended 90 day interval. Adoption of the SAP Application Security Strategy will occur July 1, 2011 and provides a solid foundation (approximately 80%) of procedural information as a starting point. Creation and/or on-going development and collection of Policies and Procedures will continue throughout the fiscal year, to be approved and adopted by the CIO by June 30, 2012.

2) Untimely employee status notification

SAP user access roles were not properly monitored.

- Forty-four of 99 users tested were improperly classified in the SAP system.
  - Five users were terminated in the HR system, but were still active in the SAP system.
  - Thirty-five users were terminated in the HR system and were locked out of SAP; however, the SAP system did not indicate that the user was terminated.
  - Four users were not properly classified as active or inactive in the SAP system.
- Twenty-five out of 164 SAP users could not be found on the HR listing. Eight of these users were not County employees; although, five of these were former SAP consultants.
- VPN access for SAP consultants was not monitored for proper use based on time restraints or module activity. SAP consultants typically have complete access to their respective modules.

Recommendation

Monthly, the ERP Manager should obtain reports from HR which identify the new employees for potential SAP access and the employee transfers or terminations affect SAP access. The HR listing should include the employee identification number, as this will ensure that SAP users are properly identified because proper names are often not used as usernames. These employee reports should be shared among ERP staff in order to proactively monitor user access.

Management Response

The ERP Manager will continue to work with the HR Department to improve/expand upon the current data interface process. As a first step, ERP was recently provided access to the HR "Termination Report" to allow for the immediate lock-out and/or removal of these affected accounts. This report will be generated and all required actions taken on a daily basis by the ERP Security staff, beginning July 1, 2011. For new hires, ERP staff will continue to work with HR to finish the development and implementation of an employee "On-Boarding" form that will be utilized to establish security roles and system access, with an anticipated "go-live" by September 30, 2011. ERP will also continue development and move toward implementation of the Move/Add/Change (MAC) Form to accommodate all employee transfers, role addition requests and change requests, i.e. name changes, etc., to begin July 1, 2011 and continue throughout the fiscal year with completion by June 30, 2012.

3) Incompatible roles existed and built-in SAP modules not utilized

Although the Business Systems Analysts (BSA) oversee user access limitation by individual users, there was no formal documentation or list of incompatible roles, and the decision of which roles are compatible or incompatible falls on individual department supervisors, IT Liaisons, and BSAs. New roles were modeled after existing employees, instead of using the system's profile generator. In addition, BSAs have unnecessary access to production roles, which creates a lack of segregation of duties, including the following:

- Five out of 56 instances in which employees had roles that were not relevant to their job description. In total, there were 22 roles incorrectly assigned to these employees.
- Two out of 25 users tested from the Accounts Payable and General Ledger modules had conflicting roles assigned in SAP.

Recommendation

The SAP program has several built-in features to assist in monitoring user access. One such feature is the Audit Information System module, which is an auditing tool designed as a centrally organized location for the audit features and functions within SAP. User access should be based on job descriptions which will help ensure that incompatible roles are not created. SAP's Profile Generator can help in this process. Default profiles should be limited to ERP security and monitored frequently. Passwords to default profiles should not be trivial, should be changed frequently and locked in a safe to ensure limited access.

Management Response

The ERP Manager, in conjunction with the ERP Technical Manager, will explore the utilization and implementation of built-in system controls, to include the expanded use of the Profile Generator tool for the creation and assignment of security roles and the use of the Audit Information System (AIS) to perform internal system and business audit controls. Additionally, ERP will transition the "approval" of roles to the applicable Department Directors, versus approval from the ERP Business System Analyst, by establishing a "User Request Form" that identifies applicable roles (with descriptions) and conflicting roles for use in Segregation of

Duties (SOD) evaluations. These steps will begin July 1, 2011 and continue throughout the fiscal year, to be completed by June 30, 2012.

* * * * *

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

July 15, 2011