SAP Follow-up
Identity and Access Management

January 2013

Steve March
Multnomah County Auditor

Audit Staff
Marc Rose
Mark Ulanowicz

Office of Multnomah County Auditor

Steve March
County Auditor

501 SE Hawthorne Room 601
Portland, Oregon 97214
Phone: (503) 988-3320

Fran Davison
Judith DeVilliers
Nicole Dewees
Craig Hunt
Jennifer McGuirk
Marc Rose
Mark Ulanowicz

Date: January 25, 2013

To: Jeff Cogen, Multnomah County Chair
Commissioners Kafoury, Smith, Shiprack, and McKeel

From: Steve March, Multnomah County Auditor
Re: SAP Follow-up: Identity & Access Management

This audit follows up our 2009 *Audit of SAP identity and Access Management* report which focused on access management and monitoring. Since that time, turnover of key personnel, changes in organizational structure, and changes in SAP architecture have significantly altered the identity and access management (IAM) landscape. While some reduction in segregation of duties conflicts has occurred, the County has taken a step backward in terms of identifying and addressing risks and in terms of defining roles and responsibilities for IAM stakeholders.

County management had not assigned ownership of the IAM process, but has now taken steps in that direction. Key stakeholders will need to work across organizational divisions and under separate leadership in order to define roles and responsibilities. It will require reaching consensus regarding which roles and combinations or roles pose the greatest risk. In addition, instituting alternative controls for known segregation of duties conflicts is needed.

Getting IAM back on track; establishing an IAM governance structure that works well; assigning clear roles and responsibilities for department managers, business process owners, and SAP/IT Security; and developing and implementing written administrative procedures to document the process will take continued effort. We appreciate the response of the Chief Operating Officer to the report and look forward to the progress to be made as a result of the steps that have been identified.

Mark Ulanowicz and Marc Rose conducted this audit. We want to thank the Department of County Management and Department of County Access staff for their assistance in this follow-up.

CC: Joanne Fuller
Sherry Swackhamer
Karyne Kieta
Mark Campbell

Table of Contents

Executive Summary

This audit is a follow-up to our 2009 report: *Audit of SAP Identity and Access Management*. In the 2009 audit, we reviewed SAP security controls to determine who had access to what information, whether that access was appropriate for the job being performed, and whether access was appropriately monitored and reported. We used the *Global Technology Audit Guide – Identity and Access Management* from the Institute of Internal Auditors as a guideline for the audit. Our recommendations from the 2009 audit focused primarily on access management and monitoring. In this follow-up, we focused on control and monitoring of privileged access and combinations of SAP roles that constitute segregation of duties conflicts.

Turnover of key personnel, changes in organizational structure, and changes in SAP architecture have significantly altered the identity and access management (IAM) landscape since the original audit. As a result, the County has taken a step backward in terms of identifying and addressing risks and in terms of defining roles and responsibilities for IAM stakeholders.

IAM stakeholders work across organizational divisions, under separate leadership, and with minimally defined roles and responsibilities. These challenges are complicated by the fact that County management has not assigned ownership of the IAM process.

Changes in the SAP system, such as the implementation of a new SAP purchasing module, have changed the business processes in these areas, as well as the risk profiles of associated SAP roles. As a result, there is no consensus regarding which roles and combinations of roles pose the greatest risk. Moreover, efforts to institute alternative controls for known segregation of duties conflicts have been inconsistent.

To get IAM back on track, management must establish an IAM governance structure; assign clear roles and responsibilities for department managers, business process owners, and IT/SAP security; and develop and implement written administrative procedures to formalize the process.

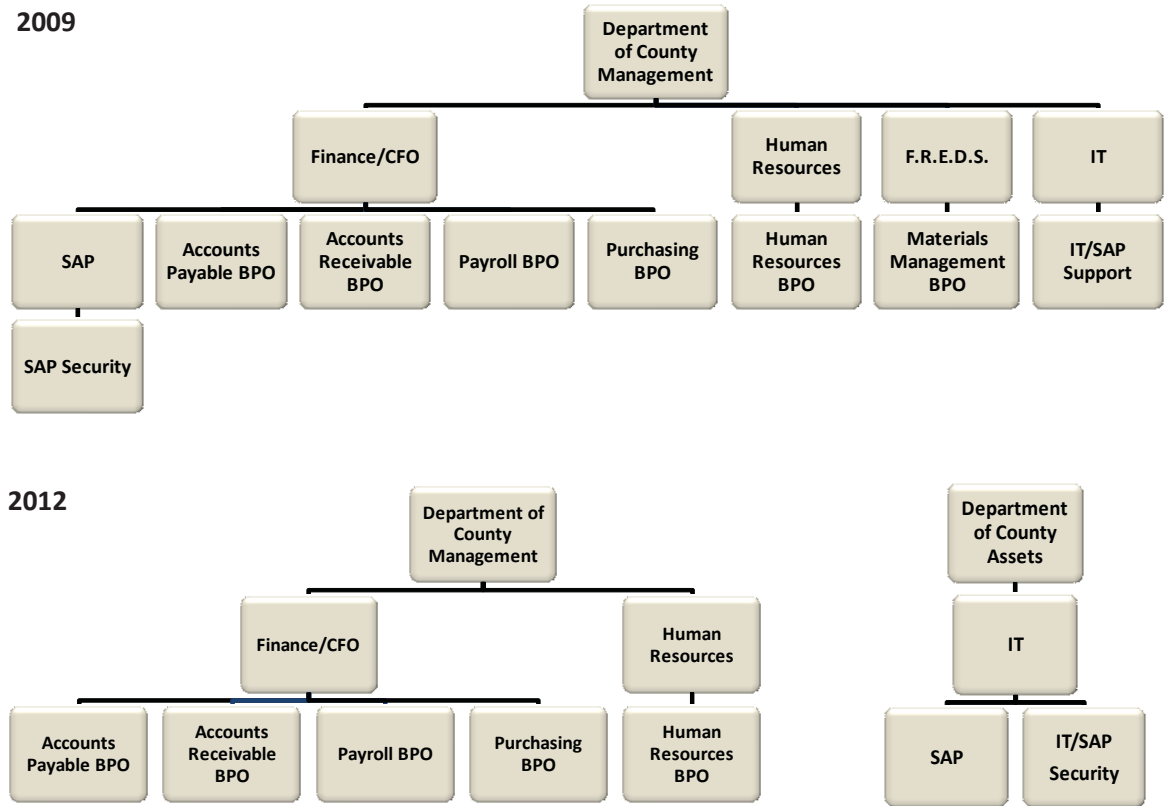
Background

Identity and access management (IAM) is the combination of policies, processes, and technology that allows for efficient and secure use of information systems. IAM is critical to Multnomah County's enterprise resource planning system, SAP, which impacts nearly all County operations, including financial accounting, contract processing, human resources, payroll, and other functions.

Employee access to SAP is based on roles linked to employee positions – the roles dictate which components of the system employees can access and which transactions they can perform. Managing SAP access is the shared responsibility of department managers, individual business process owners (BPO), and the IT/SAP security administrator. Department managers are responsible for requesting and reviewing SAP access for their staffs. BPOs are responsible for understanding and managing the functional risks of the SAP system – transactions in payroll, accounting, or human resources, for example – and for approving associated roles. The IT/SAP security administrator acts as the gatekeeper to the system and makes the actual entries into SAP to grant access.

At the time of the 2009 audit, SAP management (including SAP security) as well as all the BPOs worked under the director of the Department of County Management. At the time of this follow up, SAP management had been split into two units, SAP security and SAP application management, and moved to the newly formed Department of County Assets. Exhibit 1 below shows the change in IAM organizational structure from the 2009 to 2012.

Exhibit 1: IAM Organizational Charts 2009 and 2012



Source: Multnomah County Auditor's Office

Results

In the original audit, we identified a draft administrative procedure that detailed the roles and responsibilities of the IAM stakeholders, the process to be followed in the assignment of roles, and the process for mitigating risks associated with certain roles and combinations of roles. However, this administrative procedure was never adopted and while some of its directions have been followed, they have not been followed consistently nor have they had the force of an adopted administrative rule.

Furthermore, the turnover of key personnel, changes in the County's organizational structure, and changes in SAP architecture have significantly altered the IAM landscape since the original audit. As a result, the County has taken a step backward in terms of clearly defining roles and responsibilities for IAM stakeholders, and in identifying and addressing risks.

IAM Roles and Responsibilities

Organizational changes have had an impact on the division of responsibilities among IAM stakeholders. At the time of the original audit, the entire SAP team, as well as the majority of the BPOs, reported to the chief financial officer. SAP application management and SAP security are now in a separate County department. The reorganization highlights two fundamental weaknesses in the IAM process:

- County management has not established a governance structure for the IAM process. At the time of the original audit, IAM strategy was overseen by a steering committee, but there is no indication that this committee is still active.

- Roles and responsibilities for the IAM process are unclear. For example, there is no agreement on who is responsible for the regular review of system access, for cataloging segregation of duties conflicts and alternative controls, or for monitoring those controls.

Managing the Risks

Granting access roles to a system like SAP necessarily creates some risk. However, some roles and combinations of roles pose greater risk than others. The roles and combinations that pose the greatest risk generally fall into two categories: 1) privileged roles and 2) combinations of roles that create a segregation of duties conflict.

Privileged roles generally refer to roles used by system administrators that give them nearly unlimited ability to change system programs or data. They are necessary to perform such tasks as upgrading systems or fixing problems. These roles also give their users the ability to perform any transaction or series of transactions in the system.

Segregation of duties conflicts refer to instances where a role or combination of roles allows a single user to have control over multiple phases of a transaction. For example, a user with the ability to enter an employee's hours into the payroll system and then approve the time entry constitutes a segregation of duties conflict.

The lack of monitoring of privileged roles we identified in the original audit has essentially gone unchanged. BPOs have also granted new exceptions to segregation of duties rules since the 2009 audit without a defined process for cataloging or documenting the conflicts, leaving management with a hazy portrait of the risks those conflicts present.

Since the original audit, changes in SAP architecture and the turnover of key personnel have impacted efforts to identify roles that pose a risk.

- Changes in the SAP system, such as the implementation of a new SAP purchasing module and the elimination of some warehouse functions, have changed some of the business processes in these areas. The risk profiles of the SAP roles associated with these areas have also changed; some of the combinations of roles that constituted segregation of duties conflicts at the time of the original audit no longer pose a risk. Business process owners and IT/SAP security have not yet come to a consensus on which combinations of roles still create a segregation of duties conflict and which of these pose the greatest risks.

- The personnel responsible for overseeing SAP and SAP security have all changed. The loss of staff familiar with the SAP roles and conflicts appears to have set the process back.

- SAP management and IT/SAP security have identified an SAP report to use to review user roles and role conflicts, but have not incorporated it into a routine review process.

When IT/SAP security and/or BPOs have identified risks, there has been little consistency in mitigating the risks.

- While there has been some effort to reduce the number of existing segregation of duties conflicts, there has not been a similar effort with privileged roles. For example, there are as many user IDs with the privileged SAP_ALL developer role today as there were at the time of the original audit.

- Efforts to institute alternative controls for segregation of duties conflicts have been inconsistent.

- The 2009 audit found that department mangers did not always understand the risks related to the roles they requested for employees and our review indicates that this is still true to some extent.

Objectives Scope and Methodology

The objective of this follow-up of the *Audit of SAP Identity and Access Management* was to verify the status of its recommendations. As part of our work, we interviewed staff in SAP application management and IT/SAP security as well as business process owners. We also reviewed documentation related to segregation of duties conflicts and analyzed SAP data.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Recommendations

Effective management of the IAM process for the County's largest and arguably most important data system is critical for controlling the risk associated with the system. We recommend that County management take the following actions:

1) Establish a governance structure that takes into account the existing organizational divisions among IAM stakeholders.

2) Assign clear roles and responsibilities for department managers, business process owners, and IT/SAP security in terms of:

- requesting and granting access to the SAP system,
- routinely reviewing and documenting employees' various access levels,
- identifying and prioritizing the risks associated with various levels of access, and
- monitoring the activities of users with roles and combinations of roles that pose the greatest risk.

3) Formalize the governance structure, roles and responsibilities, and IAM processes in an administrative procedure.

Appendix

Status of Original Audit Recommendations

1a: SAP security should provide department managers and BPOs with a list of all employees who have role conflict exceptions.

Status: In Process. SAP has a report that would allow department managers and/or BPOs to identify users with specific role conflicts; however, they have not yet communicated the process to departments or BPOs. This solution also falls short of the original recommendation, in that it does not produce a list of all role conflict exceptions.

1b: Department managers need to document compensating controls for employees who have role conflict exceptions.

Status: In Process. In cases where users with role conflicts have been identified – generally in cases where new conflicting roles are requested – some BPOs require documentation of compensating controls.

1c: To retain SAP access for employees who have exceptions to identified risks, department managers need to provide documentation showing: 1) that they understand the risks involved and 2) that they have provided compensating controls or believe the risk is minimal and are willing to assume the risk.

Status: In Process. As managers request new role conflicts for their staffs, the managers who request the roles are expected to acknowledge the risk and in some, but not all cases, document how the risk associated with the role conflict will be mitigated. However, this is only the case for new requests for conflicting roles. There is no action on existing role conflicts that are not part of a new request.

1d: A list of all other department employees who have SAP access should be given to department managers on a regular basis for review to determine if the roles are still relevant for the work being done.

Status: In Process. Little or no work has been done in this area, but there have been instances where SAP management has removed unnecessary roles from some users.

2: SAP event logs should be enabled and a process for reviewing the logs should be established.

Status: In Process. SAP activated event logs for privileged developer roles, but these logs are only monitored for authentication problems - such as failed logins - which might be a sign of an attempt to hack into the system. They are not monitored for potentially improper use by privileged users.

3: Greater care is needed in assigning and monitoring roles for IT and SAP staff and for nonperson accounts.

Status: In Process. There are roughly the same number of privileged developer roles in place now as there were at the time of the original audit, including consultant and nonperson accounts.

4: Proposed administrative rules need to be completed and adopted.

Status: In Process. The draft rules that existed at the time of the original audit are being re-written.

5: The County should begin work on a single sign-on system.

Status: Not Implemented. This recommendation is considered too costly and not a high enough priority.

Response to Audit

Office of Jeff Cogen, Chair
MULTNOMAH COUNTY OREGON

501 SE Hawthorne Blvd., Suite 600
Portland, Oregon 97214
(503) 988-3308 Phone
(503) 988-3093 Fax

Date: January 17, 2013
To: Steve March, County Auditor
From: Joanne Fuller, COO
Subject: SAP Follow-up Audit

The Department of County Management (DCM) and the Department of County Assets (DCA) have received the final SAP Follow-up audit report. We appreciate the time spent by your staff on this audit and will work together to implement solutions, per your recommendations, where appropriate and cost-effective. Our overall response to your recommendations is provided below:

Follow-up SAP Audit Recommendation Overall Response:

We acknowledge that the organizational changes and turnover of key personnel that have occurred in both departments have impacted the governance structure and the associated roles and responsibilities, but be assured that both DCM and DCA understand the importance of SAP identity and access management. We are working together to formalize and document a revised governance structure that will include the associated roles and responsibilities and will be guided by the recommendations provided by the audit.

The Department of County Management, and specifically, the Chief Financial Officer (CFO) and the business process owners will have responsibility for determining proper segregation of duties when conflict of interests exists. Department management will have responsibility in their areas to document the conflicts along with the mitigating controls. A member of the CFO's staff will be assigned to oversee and monitor this process for standardization and consistency. The supporting structure will include SAP Support and SAP Security, both part of DCA's Information Technology Division who will implement SAP roles as approved by BPO's and department management. These groups will also provide support and documentation regarding SAP access, SAP role conflicts, and monitoring of both event logs and privileged access as appropriate per the recommendations from the original audit.

We would like to point out that even with the many changes that have occurred within DCM and DCA, the number of conflicting roles has been reduced by 134

conflicts or 20%. We also want to acknowledge that within DCM and DCA, establishing the DCA Administrative Hub (the Hub) resulted in the consolidation of several smaller financial operations teams from Fleet, Central Stores, Facilities and Information Technology. This has helped reduce SAP role conflicts while building stronger internal controls. The former structure was made up of small teams requiring staff to be assigned conflicting roles because there were more roles than available staff. This was especially challenging when employees were out of the office and there were even fewer staff to perform required SAP functions. Combining these teams has resulted in sufficient staffing to make discrete role assignments and afford more effective coverage for staffing absences while maintaining strong internal controls and segregation of duties.

Your findings are very thorough and we appreciate the recommendations you have made for both process improvement and strengthening internal controls.

cc: Mark Campbell, Chief Financial Officer
Sherry Swackhamer, Director, Department of County Assets