Audit of SAP
Identity and Access Management

April 2009

Craig Stroud
Multnomah County Interim Auditor

Sarah Landis
Deputy Auditor

Audit Staff
Judith DeVilliers
Mark Ulanowicz

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.

Craig Stroud
Multnomah County Interim Auditor
501 SE Hawthorne Room 601
Portland, Oregon 97214
Phone: (503) 988-3320

MEMORANDUM

Date: April 2, 2009

To: Ted Wheeler, Multnomah County Chair
Carol Ford, Department of County Management Director

From: Sarah Landis, Deputy Auditor
Judith DeVilliers, Principal Auditor
Mark Ulanowicz, Principal Auditor

Re: Audit of SAP Idenity and Access Management

The attached report covers our recent performance audit of *SAP Identity and Access Management*. As the county's enterprise resource planning system, SAP is the backbone for a variety of critical operational areas including finance, human resources, purchasing, inventory, and plant maintenance. We reviewed security controls to determine who has access to what information, whether that access was appropriate for the job being performed, and whether access and activity are appropriately monitored and reported. This report is our first of several planned audits of SAP.

We used the *Global Technology Audit Guide – Identity and Access Management* from the Institute of Internal Auditors as a guideline for the audit. We found that the SAP team was managing identity and access for the SAP system well in many areas, and has strengthened security in recent years. However, we also found that more effort was needed by the SAP team to manage potentially risky roles or combinations of roles. Department management has a role to play in necessary improvements by taking more ownership in the process of managing security through review of existing roles, removal of access when it is no longer needed, and creating and documenting controls over roles that are high risk. Increased monitoring of high risk user activity is also needed by both the SAP team and department management. Recommendations focus on addressing these concerns and building on recent and ongoing efforts by the SAP team and partners to improve SAP security.

We extend our thanks to the SAP team and department representatives for their cooperation and assistance throughout the audit and commend them for their attention to the important issue of SAP security.

Cc: Jana McLellan
Mindy Harris
Satish Nath

Table of Contents

Executive Summary

Identity and Access Management (IAM) is the combination of policies, processes, and technology that allows for efficient and secure use of an organization's information systems. While Multnomah County uses a large number of automated information systems that all require strong IAM procedures, SAP – the county's enterprise resource planning system – is the largest and arguably most complex of these systems. SAP is the county's financial system of record and contains the data necessary to run a variety of operational areas including human resources, purchasing, inventory, and plant maintenance. The importance of IAM for SAP has also been highlighted in the reports of the county's external auditor.

We used the Institute of Internal Auditors' *Global Technology Audit Guide – Identity and Access Management* (GTAG) as the primary guidelines for best practices. In applying these guidelines, we divided the IAM process into three components:

- *identity management* relates to correctly identifying the users of the system;
- *access management* relates to what information or processes an individual user can access in the system; and
- *monitoring* relates to keeping track of how individual users operate within the system.

SAP access is based on roles which are linked directly to employee positions. Managing access to SAP can be done only with close collaboration between the SAP Security Administrator, the Security Advisory Team, and county department managers. Generally, we found that the county's IAM processes for the SAP system have improved since the SAP Team took over management of SAP security. The SAP Team and IT changed the process for creating and removing employee logons and passwords. Changes have also been made in access management and monitoring, however we found additional that improvements are still needed.

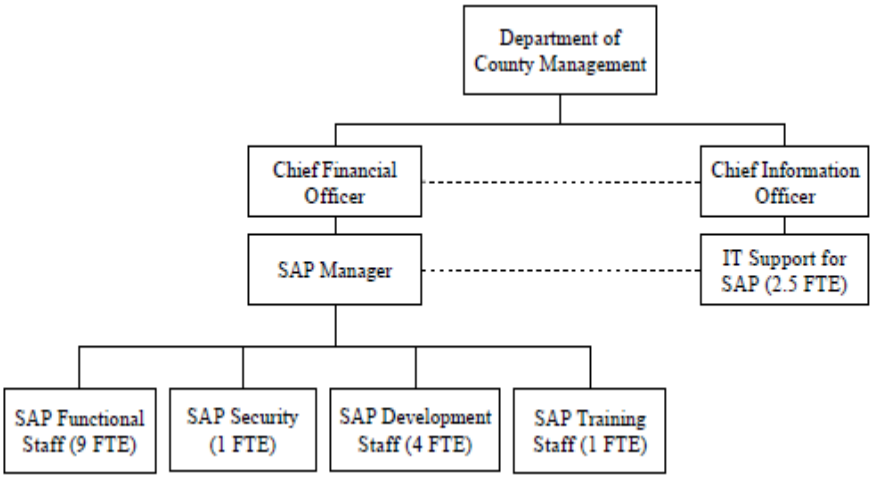
We found that the SAP Security Administrator and SAP Team need to better identify and prioritize the risks associated with various roles and combinations of roles. At the same time, department management needs to take responsibility for reviewing the existing roles they have requested for their employees, for removing access when it is not needed or used, and for documenting compensating internal controls for those employees who have been given roles identified by the SAP Team as being high-risk. Finally, the SAP Team needs to develop plans in conjunction with department management to monitor the activity of users with high-risk roles.

Background

This report is our first of several planned audits of SAP, the county's integrated information system software, which was purchased and installed in 2000. The SAP software was developed in Germany and is used by many large multi-national corporations, as well as by a number of governments.

The SAP system represents a significant county investment with a budget of $3.6 million and FTE of 17.5 for FY08. The organization chart below illustrates the way SAP is managed in the county. SAP business process functions are managed by the Chief Financial Officer (CFO), while the hardware, landscape, operating system, and technical tools are managed by the Chief Information Officer (CIO). All staff involved work in partnership and with department managers to meet the financial accounting and reporting requirements of the county. Overall SAP strategy is overseen by a steering committee which includes the CFO, CIO, Human Resources Director, and SAP Manager.

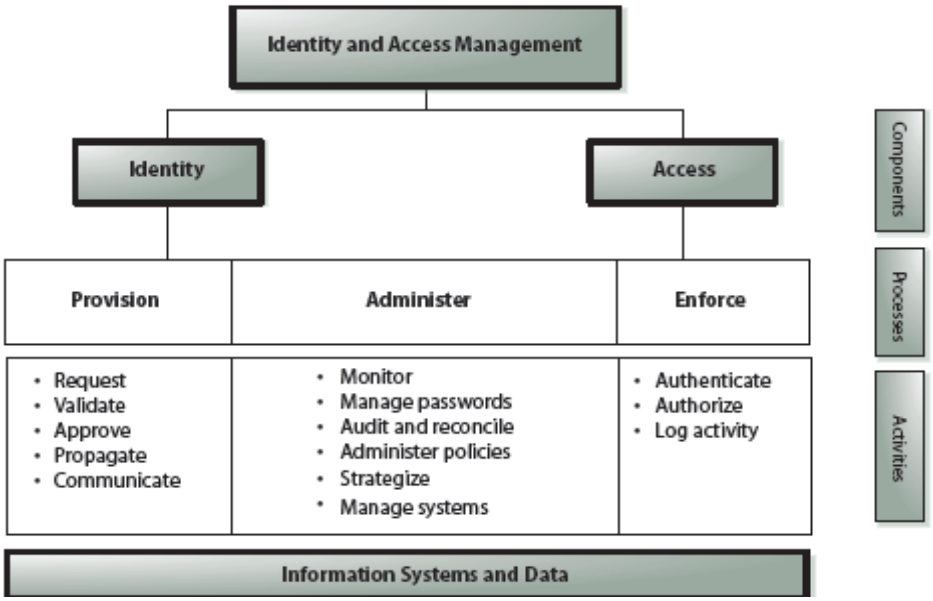
Figure 1: Organizational chart



The SAP system impacts county operations in a number of ways and is used for the county's financial accounting and payments, contract processing, budget monitoring, Human Resources (HR) and payroll, inventory management, facilities maintenance, and other functions.

Figure 2 from the GTAG audit guidelines provides an overview of the components, processes, and activities for IAM.

Figure 2: Relationships between IAM components and key concepts



Source: *Global Technology Audit Guide – Identity and Access Management* prepared by The Institute of Internal Auditors, page 5.

Provisioning (add new employees)

A request for new employee access to SAP is made by the department manager or supervisor who approves the request for access. The SAP Security Administrator gives the employee a logon name and password to get into the SAP system. The logon name is the identity part of the security system and has been strengthened over the last few years. The data and transactions to which the employee has access are the access part of the security system. For SAP security, both the identity and access are tied directly to HR master tables in the SAP system. The access, or what the employee can do in the system, is tied directly to the HR position number the employee fills. Contractor and temporary employee access to SAP is date-limited.

The SAP Security Administrator reviews the roles on the request to verify with the department requestor that the roles are still appropriate for the position and to verify continued need for any conflicting roles attached to the position. Some SAP access profiles and roles require approvals by Business Process Owners (BPOs) and department approvers who help coordinate access between SAP security and departments.

De-provisioning (employee leaves)

When an employee leaves the county or changes jobs, his or her HR position number will change and SAP access will immediately change since it is tied directly to the HR position number. The Security Administrator will de-activate the employee's SAP identity (logon and password) if the employee leaves the county. If the employee changes positions, he or she will keep the same logon; however, access to SAP will change to reflect the roles attached to the new HR position number.

Audit Scope & Methodology

We selected identity and access management as our first SAP audit because the county's external auditors have made several recommendations for improvement in this area and because it would provide us with an overview of the system and its uses. We expect to perform additional SAP-related audits, including revenues and receivables, duplicate payments, payroll, and HR, as well as reviewing current uses and needs for SAP and looking at best practices for governance.

For this audit we used the Institute of Internal Auditors' *Global Technology Audit Guide – Identity and Access Management* (GTAG) as the primary guidelines for best practices. The objectives of the audit were to determine: (1) who has access to what information; (2) whether the access is appropriate for the job being performed; and (3) if access and activity are monitored, logged, and reported appropriately.

Audit findings are based on discussions with key staff and review of pertinent documents and data. We met with Information Technology (IT) and other program managers, SAP Team staff, and other employees involved in SAP approvals and administration. We reviewed the SAP security manual and procedures and proposed administrative rules, the county's internal web page information, and best practices literature. We also analyzed SAP master tables, history tables for users, changes to user tables, roles, and changes in roles.

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.

Audit Results: Review of SAP Identity and Access Management

This section lists questions used in the IAM Guidelines from the GTAG, our findings with respect to those guidelines, and our recommendations for improvements.

#1. Is there an IAM strategy in place?

Overall SAP strategy is overseen by a steering committee which includes the CFO, CIO, HR Director, and SAP Manager. Within this context, the IAM strategy for SAP is developed and managed by the SAP Security Administrator, the SAP Team, and BPOs.

The process is documented in SAP security procedures and in the proposed administrative procedures for "SAP User Access and Role Assignment." Where applicable, the approach is consistent with IT network policies such as mandatory password changes and password format.

> ***Recommendation:*** To strengthen SAP security for IAM, the proposed administrative rules need to be completed and adopted. See recommendation #4 on page 11.

#2. Are the risks associated with the IAM process well understood by management and other relevant individuals? Are the risks addressed by the strategy?

Most of the SAP BPOs and department approvers we talked with appeared to have a good understanding of risks. Some indicated the process was cumbersome but also agreed that it was necessary and useful. Some of those responsible for approving roles indicated they could use more training and would like a better understanding of SAP roles and profiles.

We had the impression, however, that many of the department approvers did not view IAM security for SAP as part of management's internal controls for financial activity in their work areas, but rather as something technical required by "the system."

Department managers have some responsibility for SAP security and data. They request access for their employees and authorize exceptions to identified risks, such as role conflicts when employee duties are not adequately segregated.

> ***Recommendations:*** Department managers need to document compensating controls for their employees who have exceptions to identified risks. One possible way to provide this documentation would be to include it in the county's formalized internal control documentation and review process managed by the Finance Division's general ledger section, especially since SAP security and controls are integral to the financial system and reporting.
>
> To retain SAP access for employees who have exceptions to identified risks, department managers need to provide this documentation to the SAP Security Administrator showing (1) that they understand the risks related to these roles (2) that they have provided compensating controls to mitigate that risk, or (3) that they believe the internal control risks are minimal and that they are willing assume the identified risks. See recommendation #1b and #1c on page 11.

#3. Are there defined methods to appropriately account for issues related to segregation of duties?

Segregation of duties is an internal control intended to prevent or decrease the occurrence of innocent errors or intentional fraud. This is done by ensuring that no single individual has control over all phases of a transaction. There are four general categories of duties: authorization,

custody, record keeping, and reconciliation. In an ideal system, different employees perform each of these four major functions. In other words, no one person has control of two or more of these responsibilities.

When SAP was implemented, consultants hired by the county created a list of identified role conflicts which is used as criteria in assigning roles. The SAP Team indicated that the risks related to conflicts in some instances are much lower than for other instances. In the past, the review of possible conflicting roles was not part of the process for granting employees roles or changes to roles. There is now a large number, 229 or 19% of current users, who have conflicting roles. Although the recently adopted process requires the SAP Security Administrator to check new role assignments against this list, we found few instances where this check was done in our review of a sample of role assignments.

In talking with department managers, we found that they do not always have a good understanding of the risks related to some of the roles they request for their employees. Some said they rely on the interaction with the Security Administrator and Advisory Team. Many department managers indicated that exceptions are needed for allowing conflicting roles in some instances, such as when employees are geographically separated in smaller office settings.

The risks related to employees who have been given exceptions and allowed to have SAP roles which are identified as being in conflict, are even greater because these roles, once allowed, are not reviewed or monitored. Regular review and monitoring helps ensure that roles are still needed and that the department has other compensating controls to mitigate risks where segregation of duties has been compromised.

> ***Recommendation:*** To improve IAM security, additional review and monitoring of employee access to SAP is needed. This should include a routine review of roles given to employees and more frequent review where exceptions have been granted, such as in the case of conflicting roles or roles that allow individuals greater ability to access or change data in the system. See recommendation #1a – 1d on page 11.

#4. Is the IAM environment centralized or distributed appropriately to reflect the structure of the organization?

An ideal technical situation would be to have a "single software" solution with consistent processes clearly documented and managed through a single implementation tool. According to best practices, a single software solution for single sign-on is both effective and efficient. Single sign-on means a user has only one user identification and password (identity management) which gives him or her access to all software applications and permissions (access management) for which the user has been approved.

The county does not have a single software solution for IAM and each software application is managed separately.

> ***Recommendation:*** To better align with IAM best practices and improve both efficiency and effectiveness for IAM security countywide, the county should begin work on the development of a single sign-on system. See recommendation #5 on page 11.

#5. How are password policies established, and are they sufficient for the organization?

Policies that govern IAM processes are critical components of any effective system. Password policies for SAP have improved over the last few years and now follow the network policy for mandatory password changes every 90 days and carry the same format requirements. In addition, SAP Security uses a feature in SAP to generate random passwords for a new user's initial password or password reset.

SAP security procedures are also available on the county's internal web site to communicate password policies to the employees.

Recommendation: None

#6. Does the organization have consistent processes for managing system access?

As part of our review we observed the process for adding users and roles and reviewed supporting documentation for a sample of users. We found that there is a consistent process for managing system access which is communicated to users on the county's internal web site and in proposed administrative rules. SAP Security has a procedures manual, which allows for consistency when the Security Administrator is not available.

BPOs and department approvers are aware of procedures and have reported that they rely on the Security Administrator and SAP Team and to provide them information they need to do their jobs.

Recommendation: None

#7. Can auditors identify the unique individuals who are granted access to the organization's systems based on the sign-on credentials they are assigned?

We were able to identify all SAP users by using the SAP system. We looked at SAP master tables and history tables for users, passwords, roles, and permissions to identify users and their access. We created a random sample of users and traced them to original authorization documents.

Recommendation: None

#8. Is employee productivity degraded because it is too difficult to gain and maintain system access?

We interviewed both BPOs and department approvers. Although some thought the process was cumbersome, they also agreed it was necessary. None of those we spoke with thought employee productivity was degraded because it was difficult to access the system.

Recommendation: None

#9. Who should approve access for a user in the environment?

The approval process includes multiple people: department managers, department approvers, BPOs, and the SAP Security Administrator.

The SAP Security Administrator and BPOs rely on the knowledge of department managers who request access to the system and who know and understand the needs of employees doing the work. At the same time, the department managers rely on the BPOs and the SAP Security Administrator to understand the effects and risks for each access role granted in the system (i.e. what that employee can "do" in the system).

Some of the managers we talked with thought they could use more information about the risks in the roles they were requesting. However most thought the SAP Team answered their questions and worked with them to ensure access was appropriate.

Recommendation: None

#10. Can the organization demonstrate that only appropriate people have access to information?

For the last three years, the county's external auditors have reviewed the SAP system and each year recommended the county review users and roles. The objective of such a review would be to verify that only the appropriate people have access to information and whether roles assigned to positions are still necessary for the information needs and duties of that position.

We were told such a review would be time consuming, especially for department management. However, there may be a risk that inappropriate employees have access to SAP data for the following reasons: 1) SAP security in prior years was not as well managed as it is currently; 2) needs and duties for positions have changed over the years; and 3) there has not been a complete review of users or their access needs, especially for those whose access and roles were granted prior to current practice.

> ***Recommendation:*** To improve IAM security, additional review and monitoring of employee access to SAP is needed. This should include a routine review of roles given to employees and more frequent review where exceptions have been granted, such as in the case of conflicting roles or roles that allow individuals greater ability to access or change data in the system. See recommendation #1a – 1d on page 11.

#11. Are there appropriate controls in place to prevent people from adding access to systems and applications outside the approved process?

According to management, the ability to add, modify, or delete SAP users is limited because SAP security roles have been assigned to only three SAP employees and two IT database administrators. There is also a policy that does not allow SAP or IT employees to create their own roles and access.

However, during our review of the "Change History for Authorizations" table in SAP, we found instances where the SAP Team and IT have modified their own roles. This lack of control creates an even greater risk because there is no monitoring or review of users to trace their access in the system.

> ***Recommendation:*** To improve security, greater care is needed in assigning and monitoring roles for IT and SAP staff and for nonperson accounts, especially for the more powerful privileged roles. All changes in roles of IT and SAP staff and for nonperson accounts should be documented and approved. The SAP Security Administrator should monitor who has made changes to user roles by reviewing the "Change History for Authorizations" table on a regular basis. See recommendation #3 on page 11.

#12. When people leave the organization, does it identify what system access they have and revoke it in a timely manner?

IAM audits often find that users retain access to accounts long after they leave an organization. The risk that terminated employees could still have access to the SAP system is lessened because the SAP process for IAM is tied directly to the HR system.

When an employee leaves the county or a specific position in the county, his or her access to the SAP roles attached to that position are automatically terminated. The SAP Security Administrator runs a weekly termination report for SAP users who leave county employment; this report is used to remove the user identification (logon) from the master tables.

Revocation for non-employees, such as contractors or temporary employees, is based on a predetermined termination date put into the system when their roles are originally approved. We reviewed master tables and found no issues.

Recommendation: None

#13. What does the organization do with respect to nonperson accounts?

Nonperson accounts are not associated with a particular employee logon. These types of accounts are needed for system interfaces or processes. An example of a nonperson account would be a batch account used to produce scheduled reports. SAP security policy has changed in how nonperson accounts are handled and, according to SAP management, they will continue limiting the access and use of these type of accounts.

Because nonperson accounts generally have higher access privileges, extra care is needed to document the reason and authorization for these accounts. Such accounts also need to be frequently reviewed.

Recommendation: To improve security, greater care is needed in assigning and monitoring roles for IT and SAP staff and for nonperson accounts, especially for the more powerful privileged roles. All changes in the roles of IT and SAP staff and for nonperson accounts should be documented and approved. The SAP Security Administrator should monitor who has made changes to user roles by reviewing the "Change History for Authorizations" table on a regular basis. See recommendation #3 on page 11.

#14. What does the organization do with respect to privileged accounts?

Privileged accounts generally refer to those used by administrative accounts and users that allow unlimited ability to change programs or data. We found improvements over the controls for administrative privilege and that the number of these roles has decreased significantly since 2006.

Other privileged accounts include those for users who have more powerful roles or a larger number of roles, allowing greater access to data or to the ability to change data than is given to most users. We found that 57 current users (5.4% of the total) have over 30 profiles, which are summaries of roles, while 71% of the users have 15 or fewer profiles. Sometimes a position is given additional roles for various purposes, such as a special project. Because roles are not reviewed and deleted when no longer needed, some users may have access to more information than is needed to do their jobs. User accounts with more profiles or privileges are a greater risk and should be monitored more closely than other user accounts.

Recommendations: To improve IAM security, additional review and monitoring of employee access to SAP is needed. This should include a routine review of roles given to employees and more frequent review where exceptions have been granted, such as in the case of conflicting roles or roles that allow individuals greater ability to access or change data in the system. See recommendation #1a – 1d on page 11.

Greater care is needed in assigning and monitoring roles for IT and SAP staff and for nonperson accounts, especially for the more powerful privileged roles. All changes in roles to IT and SAP staff and for nonperson accounts should be documented and approved. The SAP Security Administrator should monitor who has made changes to user roles by reviewing the "Change History for Authorizations" table on a regular basis. See recommendation #3 on page 11.

#15. How strong are the controls in place to prevent people from bypassing authentication or authorization controls?

SAP as a system has strong internal controls which prevent users from bypassing authentication or authorization controls. We found that controls over passwords have been strengthened over the last few years. Additional protection is afforded in that the system cannot be accessed by users outside of the Local Area Network environment, which provides additional authentication security.

Recommendation: None

#16. How is information logged, collected, and reviewed?

Enabling event logging has been a recommendation by the county's external auditors for three years. Security event logging, along with regular reviews of these logs, can reveal if breaches or attempted breaches of the system have occurred. According to SAP management, they have begun to implement event logging as of this report.

Recommendation: Event logging in SAP should be enabled and a process for reviewing the logs established. See recommendation #2 on page 11.

Audit Recommendations

1 - To improve IAM security, additional review and monitoring of employee access to SAP is needed. This should include a routine review of roles given to employees and more frequent review where exceptions have been granted, such as in the case of conflicting roles or roles that allow individuals greater ability to access or change data in the system:

> 1a - At least annually, or more frequently if needed, the SAP Security Administrator should provide department managers and BPOs with a list of all employees who have been allowed exceptions to security standards. Examples of exceptions include: employees who are allowed SAP roles that, when combined, create a conflict of interest; those who have a large number of roles; those who are given more powerful roles; and any other criteria the SAP Security Advisory Committee believes have some risks and should limited and be subject to additional monitoring.
>
> 1b – Department managers need to document compensating controls for employees who have exceptions to identified risks. One possible way to provide this documentation would be to include it in the county's formalized internal control documentation and review process managed by the Finance Division's general ledger section, especially since SAP security and controls are integral to the financial system and reporting.
>
> 1c - To retain SAP access for employees who have exceptions to identified risks, department managers need to provide documentation to the SAP security administrator showing (1) that they understand the risks related to these roles, (2) that they have provided compensating controls to mitigate that risk, or (3) that they believe the internal control risks are minimal and that they are willing assume the identified risks.
>
> 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 on the position are still relevant to the work being done. If not, those excess roles should be eliminated.

2 - To improve security, the SAP event logs should be enabled and a process for reviewing the logs should be established.

3 - To improve security, greater care is needed in assigning and monitoring roles for IT and SAP staff and for nonperson accounts, especially for the more powerful privileged roles. All changes in roles to IT and SAP staff and for nonperson accounts should be documented and approved. The SAP Security Administrator should monitor who has made changes to user roles by reviewing the "Change History for Authorizations" table on a regular basis.

4 - To strengthen SAP security for IAM, the proposed administrative rules need to be completed and adopted.

5 - To better align with IAM best practices and improve both efficiency and effectiveness for IAM security countywide, the county should begin work on the development of a single sign-on system.

Response to the Audit

Department of County Management
MULTNOMAH COUNTY OREGON
501 SE Hawthorne, Suite 531
Portland, Oregon 97214-3501
(503) 988-3312 phone
(503) 988-3292 fax

To: Sarah Landis, Deputy Auditor
Judith DeVilliers, Principal Auditor
Mark Ulanowicz, Principal Auditor

From: Carol Ford, Department of County Management Director
Mindy Harris, Chief Financial Officer

Date: March 27, 2009

Re: Final Draft of the SAP Identity and Access Management Audit

The Department of County Management and the Finance and Risk Management Division appreciate the time that you and your staff have invested in the review of the SAP Access and Identity Management. We would like to thank you for the thoughtful recommendations and thorough audit. We appreciate the opportunity to comment on your findings and recommendations.

The SAP Support Team is continuing to pursue several initiatives that will address many of the recommendations noted in your report. Specifically, SAP is working on increasing the SAP role review at the central level as well as at the Departmental level. In addition by June 30, 2009, we anticipate completing a County-wide Administrative Procedure that will stress the importance of SAP security and require standard security procedures. We have prepared a more detailed plan addressing many of the concerns noted in your report, including SAP role-conflicts, a single sign-on system, increased education and training on SAP roles and installing an SAP application to help manage and mitigate role risks. We would also like to note that the SAP Support Team has already implemented "Event Logging" as recommended by our external auditors, Moss Adams, in their IT review report from the June 30, 2008 audit.

We agree with your recommendations and appreciate the time and effort taken to compile this report. The recommendations will assist us in improving and strengthening the County's system of record as it relates to identify and access management. We would be happy to provide your office with progress updates as we address and implement the recommendations.

cc: Satish Nath, SAP Manager
Cara Fitzpatrick, Accounting Manager

Multnomah County Auditor
501 SE Hawthorne, Room 601
Portland, Oregon 97214
503-988-3320
www.co.multnomah.or.us/auditor

The Multnomah County Auditor's Office launched the **Good Government Hotline** in October 2007 to provide a mechanism for the public and county employees to report concerns about fraud, abuse of position, and waste of resources.

The **Good Government Hotline** is available **24 hours a day, seven days a week.** Go to GoodGovHotline.com or call 1-888-289-6839 for more information or to make a report.