Steve March
Multnomah County Auditor
501 S.E. Hawthorne
Portland, Oregon 97214
Telephone 503-988-3320
www.multco.us/auditor

Unclear Identity and Access Management Puts County at Unnecessary Risk: Second follow-up on SAP IAM

Jennifer McGuirk, Senior Management Auditor
Marc Rose, Senior Management Auditor

Executive Summary

Identity and Access Management (IAM) is important to safeguarding the sensitive personal and financial information entrusted to Multnomah County. Accordingly, the Auditor's Office audited IAM for the County's enterprise system, SAP, in 2009 and in a 2013 follow-up audit. In this audit, we assessed the status of recommendations from our 2013 SAP IAM follow-up.

We found that the County still needs to fully implement our 2013 follow-up recommendations. However, we did find some movement to improve IAM. The County has brought a critical SAP role back in-house; the recently hired SAP Security Administrator is a County employee as opposed to a contractor. This should help reduce the previous annual turnover in that role. In addition, there appeared to be some progress to reduce conflicts and increase monitoring.

While these steps are promising, they do not appear to address root causes of the County's IAM challenges. The underlying challenges to effective IAM implementation appear to be a lack of collaboration among stakeholders and a lack of ownership of the process. Notably, a governance structure has not been established, and roles and responsibilities remain murky, leaving gaps in the County's ability to identify risks and monitor for fraud or error.

Since effective IAM is critical to protect the County's personal and financial data, it is essential that County management prioritize SAP IAM, assign leadership, and promote collaboration. We recommend the following:

1) Strong executive leadership is necessary to promote the importance of IAM and propel the vision and plan for its implementation. The County should identify an executive sponsor for IAM.
2) The County, through the executive sponsor, should articulate a plan to establish a governance structure and address the 2013 audit recommendations. The plan should include identifying a team leader who can work collaboratively and span the IT-business units divide.
3) The County should inventory current monitoring practices and identify gaps that could allow for loss and/or liability.

Previous IAM Audit Results

The genesis of this audit was our 2009 *Audit of SAP Identity and Access Management*. The 2009 audit reviewed SAP security controls to determine who had access to what information, whether that access was appropriate, and whether access was appropriately monitored and reported. We completed a follow-up audit in 2013, and focused on control and monitoring of privileged roles, as well as combinations of SAP roles that constituted segregation of duties conflicts. The follow-up audit revealed that the County had taken a step backward in terms of identifying risks and defining roles and responsibilities for IAM stakeholders.

In the 2013 follow-up audit, we provided three primary recommendations: establish a governance structure; assign clear roles and responsibilities for stakeholders; and develop and implement written administrative procedures to formalize the process. Since 2013, the County has reduced the number of identified role conflicts that could allow a user to mistakenly or fraudulently compromise SAP data and has increased monitoring to some extent. However, IAM for SAP remains somewhat scattered and ad-hoc, with stakeholders acting primarily in silos rather than in the coordinated fashion that is necessary for effective IAM. Furthermore, the role conflict matrix has evolved over time and is not necessarily a comprehensive list of conflicts.

Why Identity and Access Management Matters

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, compliance with privacy regulations, and other functions.

IAM matters regardless of the enterprise resource planning system that an organization uses. Effective IAM can enhance business process efficiency while reducing the risk of financial loss due to fraud,

Some Key County IAM Terms

- **Business Process Owners**: Senior County employees 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.

- **Position**: Access to SAP is based on roles linked to employee positions. Roles are not linked to individuals. This means that when an employee starts in a position, he/she inherits the roles already approved for that position.

- **Privileged role**: Generally, a system administrator role that gives nearly unlimited ability to change system programs or data. Monitoring is important to ensure these roles are used appropriately.

- **Role**: Roles dictate what a position can access and which transactions it can perform.

- **Role conflict matrix**: The County's Excel matrix that documents high-risk role conflicts. The matrix is to be used to prevent approving conflicting roles for a position, except as necessary to perform essential job functions.

- **Segregation of duties conflict**: An instance where a position has a role or combination of roles that allows the control of multiple phases of a transaction, such as creating and paying an invoice. In some cases, it is necessary for a position to have conflicting roles. Monitoring is important to ensure a position does not use conflicting roles within a transaction.

mistake, or data breach. The typical business can expect to lose 5% of its revenues to fraud. Data breaches, in which personal or financial data are compromised, are increasing in frequency. A recent case involving the breach of up to 4 million federal employees' personal information could cost the federal government $20 million. While no system can eliminate the potential for fraud or a data breach, effective IAM improves risk posture by providing a framework to safeguard and monitor access to financial and personal data.

What We Found

The County still needs to fully implement the recommendations from the 2013 follow-up. However, we did find some movement to improve IAM. The County has brought a critical SAP role back in-house; the recently hired SAP Security Administrator is a County employee as opposed to a contractor, which should help reduce the previous annual turnover in that role. In addition, there appeared to be efforts to address role conflicts, and to improve collaboration among key stakeholders. While these steps are promising, they do not appear to address root causes of the County's IAM challenges.

Governance Structure – Needs to be established.

We noted in our prior follow-up audit some of the challenging conditions faced by the County in regard to IAM: the primary stakeholders, SAP/IT Security and business process owners, work across organizational divisions, under separate leadership, and with minimally defined roles and responsibilities; and County management has not assigned ownership of the IAM process. We expected that the establishment of a governance structure would mitigate and meet these challenging conditions. However, we found that these conditions remain and the governance structure has not been established.

One of the essential elements of a governance structure for IAM is collaboration. Collaboration helps address the gap that often exists between those on the technical side of the process (IT), and those on the business side (business process owners and business/department managers).
Successful collaboration depends on executive leadership and on a team leader with strong communication skills.

- **The role of the executive sponsor:** Best practices describe an executive sponsor as essential to effective IAM. An executive sponsor ensures IAM is an organizational priority—one that has the necessary resources and active participation of stakeholders. Executive sponsors can motivate the team, build stakeholder consensus, and ensure stakeholder accountability and adherence to expectations.
- **The role of the team leader:** The team leader could also be considered the program manager. Ideally, this person demonstrates business and technical skills that help ensure IAM meets organizational objectives and is successfully implemented. These skills also help team leaders communicate effectively among IAM's diverse stakeholders. Team leaders advocate for and manage change, and help create buy-in across the organization for how it will handle IAM.

According to best practices, a typical IAM team would resemble the group shown in Exhibit 1.

1. Executive Sponsor
2. Team Leader
3. IT and Security
4. Business Managers
5. Business Application Owners
6. Operation Risk Managers
7. Human Resources

We found that some individuals or groups represented in Exhibit 1 have worked on IAM tasks. For example, senior County employees in finance and risk have participated in role review. But notably, we could not identify an official team, an executive sponsor, or a team leader.

In addition, overall IAM work has not necessarily been coordinated; stakeholders have essentially worked in silos. Not all stakeholders had the same knowledge about major tasks, which suggested a significant need to improve communication, as well as the continuing need for a governance structure.

Clear Roles and Responsibilities – Need to be assigned.

We found that stakeholders have continued to fulfill similar roles as they did at the time of the 2013 follow-up audit. Some stakeholders have taken on additional tasks to increase monitoring and identify risks, and some have worked together to refine the list of conflicts. However, these efforts appear more ad-hoc than as part of an intentional plan, and have been rolled out in limited circumstances.

Monitoring is critical to IAM, for it helps ensure the accountability of transactions run through privileged user accounts, and for users with conflicting roles (roles that create a segregation of duties conflict). A lack of adequate monitoring could permit a mistake or fraudulent transaction to go unnoticed, exposing the County to great potential compromise of protected information, financial loss, or loss of reputation. A recent attack on federal government computer systems compromised the financial and/or personal information of up to four million employees, which hackers exploited by gaining privileged user access.

The monitoring tasks, though increased, were not prescribed in any documentation that we viewed, and it was difficult to determine how frequently the tasks were expected to be completed. In addition, while some business process owners had access to monitoring reports that can be regularly generated to look for suspect transactions, others did not.

The process for identifying and prioritizing the risks associated with various levels of access is not defined. Best practices suggest that the business process owners should be responsible for identifying the business risks and the necessary segregation of duties, while IT staff will typically have the technical expertise to identify SAP role conflicts. This requires collaboration. We saw limited examples of this kind of collaboration in a project to reevaluate the risk matrix and in a payroll project to identify role conflicts, but the ownership of similar future work appears uncertain.

Administrative Procedure – Key stakeholders need to be involved.

The Identity and Access Management Administrative Procedure is awaiting senior management approval. We found that some of the business process owners were unfamiliar with or unaware of the written procedure. Given that they understand the business risks and the associated segregation of duties controls, the business process owners should have been involved in drafting the procedure. The procedure, more importantly, appears to put the cart in front of the horse. As noted previously, the IAM governance structure has not been established, nor has an overall plan been articulated that takes into account the needs and abilities of the various stakeholders. In our opinion, the draft administrative procedure needs to be revisited to ensure all key stakeholders have an opportunity for review and input.

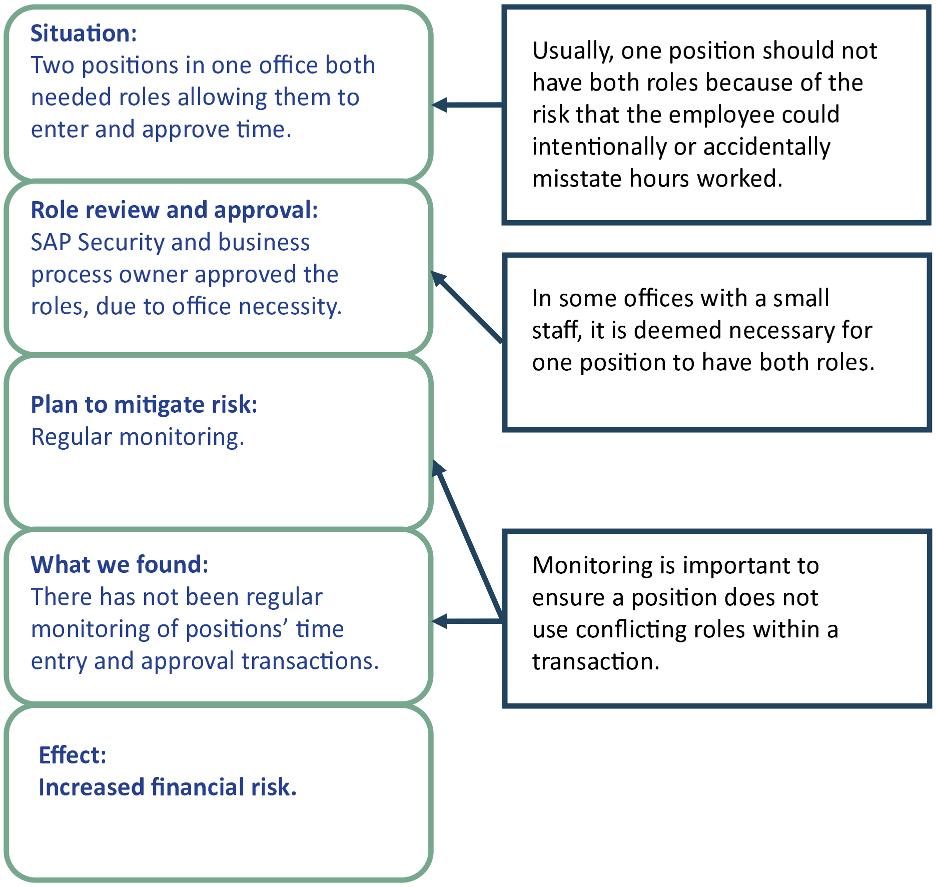
What is the effect? Unclear IAM puts the County at unnecessary risk.

As described above, a great deal of ambiguity surrounds IAM. This ambiguity makes it difficult, if not impossible, to hold individuals accountable for IAM tasks—because it is not clear who is responsible.

Ambiguous roles and responsibilities lead to at least two possibilities: (1) Work is being duplicated unbeknownst to the people doing the work, which is inefficient, and/or, (2) important monitoring or conflict analysis is not being done, under the false assumption that someone else is doing it. When this work doesn’t happen, it increases the likelihood for personal and financial data to be compromised.

Exhibit 2 below shows an example of a role conflict that managers approved but that has not been adequately monitored, which increases the risk of the County losing money to fraud or error.

Exhibit 2. Irregular monitoring of an identified role conflict increases risk



Situation:
Two positions in one office both needed roles allowing them to enter and approve time.

Usually, one position should not have both roles because of the risk that the employee could intentionally or accidentally misstate hours worked.

Role review and approval:
SAP Security and business process owner approved the roles, due to office necessity.

In some offices with a small staff, it is deemed necessary for one position to have both roles.

Plan to mitigate risk:
Regular monitoring.

What we found:
There has not been regular monitoring of positions’ time entry and approval transactions.

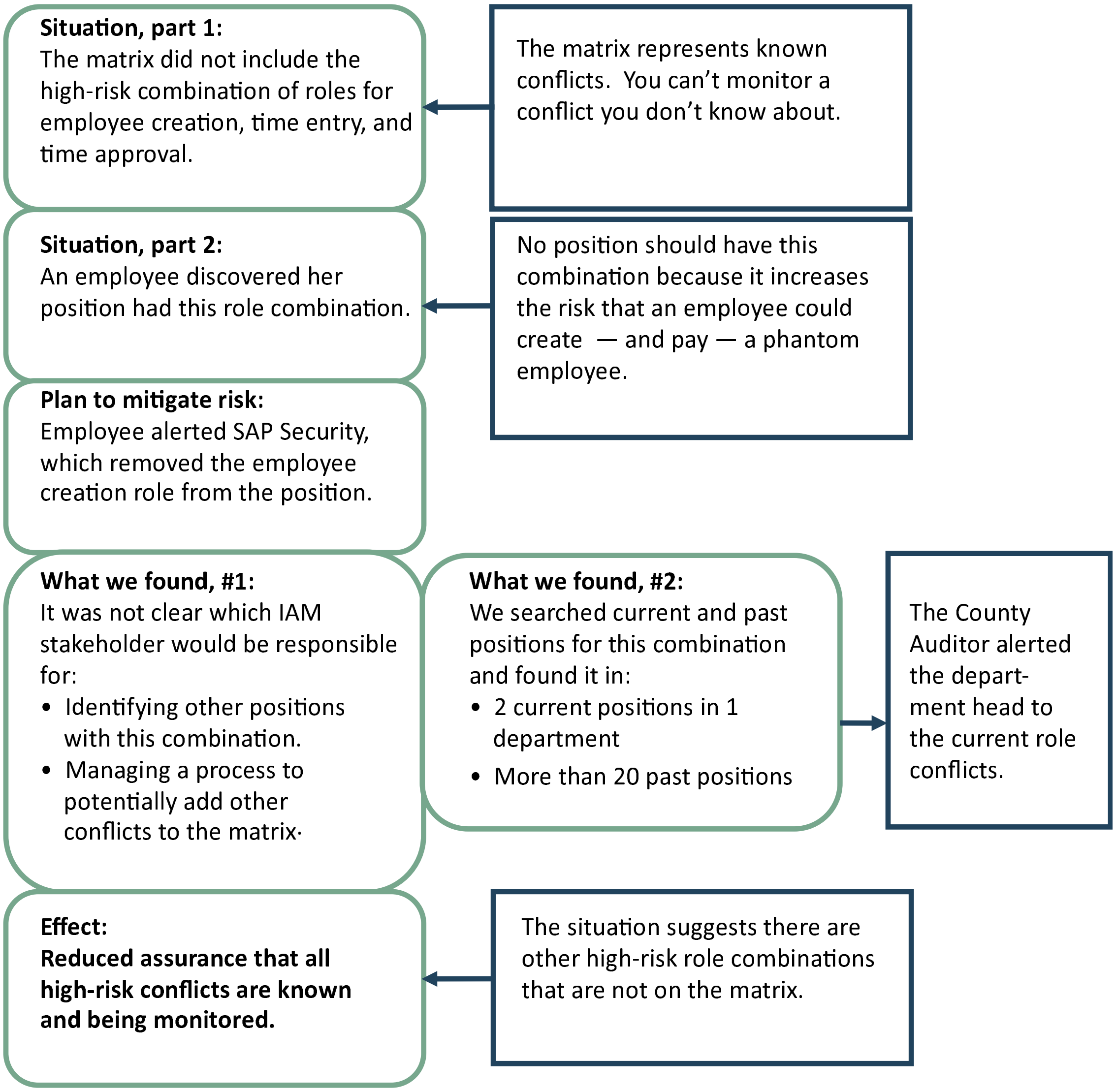
Monitoring is important to ensure a position does not use conflicting roles within a transaction.

Effect:
Increased financial risk.

Source: Auditor’s Office

A lack of monitoring altogether also poses risk to the County. During the time of our audit, an employee revealed to us that she recently realized she had the combination of roles necessary to create *and* pay an employee – a combination that no one in the organization should have, and which was not included on the conflict matrix. Exhibit 3 describes the situation.

Exhibit 3. Discovery of a high-risk conflict not on County's role conflict matrix reduces assurance that all high-risk conflicts are known, monitored



Situation, part 1:
The matrix did not include the high-risk combination of roles for employee creation, time entry, and time approval.

The matrix represents known conflicts. You can't monitor a conflict you don't know about.

Situation, part 2:
An employee discovered her position had this role combination.

No position should have this combination because it increases the risk that an employee could create — and pay — a phantom employee.

Plan to mitigate risk:
Employee alerted SAP Security, which removed the employee creation role from the position.

What we found, #1:
It was not clear which IAM stakeholder would be responsible for:

- Identifying other positions with this combination.
- Managing a process to potentially add other conflicts to the matrix·

What we found, #2:
We searched current and past positions for this combination and found it in:

- 2 current positions in 1 department
- More than 20 past positions

The County Auditor alerted the department head to the current role conflicts.

Effect:
Reduced assurance that all high-risk conflicts are known and being monitored.

The situation suggests there are other high-risk role combinations that are not on the matrix.

Source: Auditor's Office

The discovery of the conflict in Exhibit 3 suggests there are others that remain unknown. The following recommendations are intended to improve IAM and the County's risk posture.

Recommendations

1) Strong executive leadership is necessary to promote the importance of Identity and Access Management and propel the vision and plan for its implementation. The County should identify an executive sponsor for IAM.
2) The County, through the executive sponsor, should articulate a plan to establish a governance structure and address the 2013 audit recommendations. The plan should include identifying a team leader who can work collaboratively and span the IT-business units divide.
3) The County should inventory current monitoring practices and identify gaps that could allow for loss and/or liability.

Objectives, Scope, and Methodology

The objective of this follow-up audit was to assess the status of recommendations from our 2013 SAP IAM follow-up. Our work included interviewing current and former business process owners, as well as staff in SAP application management and IT/SAP Security. We also reviewed IAM best practices, analyzed SAP data, and reviewed reports on privileged roles and segregation of duties conflicts. We focused on the time period following the 2013 audit through May 2015, with one exception. During the course of the audit, an employee revealed that she recently realized she had the combination of roles necessary to create and pay an employee – a combination that no one in the organization should have, and which was not included on the County's role conflict matrix. Accordingly, we conducted a historical analysis of this role combination using SAP data.

We conducted this 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Department of County Management

Multnomah County

Office of the Chief Operating Officer

September 11, 2015

Auditor Steve March
501 SE Hawthorne Blvd, Ste 600
Portland, OR 97206

Dear Auditor March:

Thank you for the opportunity to review and comment on the SAP Identity and Access Management Audit. Identity and Access Management (IAM) is a vital component in the effort to safeguard and protect the County's personal and financial data. The 2009 audit of SAP, conducted by your office, as well as the 2013 follow-up audit, documented several critical areas that need to be improved. We agree with the findings, and have established that the following areas will be addressed:

- We agree that strong executive leadership is necessary to promote the importance of IAM and propel the vision and plan for its implementation. We will identify an executive sponsor for IAM.
- We agree that, through the executive sponsor, a plan to establish a governance structure should be created, and that it must address the 2013 audit recommendations. In addition, we agree that a team leader should be identified who can work collaboratively and span the IT - business unit divide.
- We agree that our current monitoring practices must be inventoried and gaps that could allow for loss and / or liability identified.

The 2013 follow-up audit provided three primary recommendations: establish a governance structure; assign clear roles and responsibilities for stakeholders; and develop and implement written administrative procedures to formalize the process. We believe we have taken steps to reduce the number of identified role conflicts that could allow a user to mistakenly or fraudulently compromise SAP data and we have increased monitoring. We are now poised to take the steps necessary to provide the coordinated activities required for effective identity and access management.

I am pleased to confirm that I will serve as the Executive Sponsor for IAM. I have asked Bob Leek, Multnomah County Deputy CIO, to serve as the Team Leader and to work collaboratively with all of the key stakeholders, including IT Security and SAP team members, Business Process Owners, Business Application Owners, and Department members to address the improvements needed in IAM. That team will propose a governance structure to oversee the creation of recommendations for administrative procedures to formalize processes.

We agree that IAM, as a combination of policies, processes, and technology, will allow for efficient and secure use of the SAP information system, a critical tool that impacts nearly all of County operations. Thank you for your vigilance in continuing to drawing attention to this critical area and for helping us identify measures we can take to proactively address the root causes of the County's IAM challenges. I look forward to sharing our future progress.

Sincerely,

Marissa Madrigal
Chief Operating Officer