Performance Audit

SAP
Identity and Access Management

Durham County Internal Audit Department

May 21, 2010

EXECUTIVE SUMMARY

May 21, 2010

Durham County
Internal Audit Department
(919) 560-0042

Performance Audit:

SAP Identification and Access Management

Why We Did This Audit

This audit was conducted to examine the strength of Identification and Access Management (IAM) controls in SAP, the County's Enterprise Resource Planning (ERP) system. IAM is a mechanism to assure controls are adequate to safeguard the County's proprietary information as well as bring about business efficiencies, effectiveness, and compliance. Specific audit questions were to determine:

1. If access authorization methods are appropriate to assure that only those needing access are granted access,
2. Who has access to specific SAP information and is the access authorization justifiable for the task, and
3. Is access and activity monitored, logged, and reported in according with best practices?

What Is Recommended

The recommendations address an authority for development and implementation of policies and procedures. Policies and procedures set the groundwork to (a) monitor what information and processes an individual user can access and (b) keep track of how individual users operate with the system. Upon designation by the County Manager as lead SAP user administrator, we recommend that SAP Shared Services:

1. Develop formal policies and procedures to provide guidance to SAP Subject Matter Experts (SMEs) and departmental users to monitor entitlement permission appropriateness.
2. Develop and communicate to users a system for monitoring user accounts.
3. Develop a system to track compliance with policies and procedures.
4. Provide instructions for handling segregation of duty conflicts in formal policy and procedures documents.

What we found

Although SAP Shared Services has the tools, it has not been designated the responsible entity for overseeing SAP activities at the user level. It is primarily the administrators of software programs that make up the system and acts as the repository of entitlement permissions information. Shared Services work with a group of Subject Matter Experts to provide system access.

The County has operated without formal policies and procedures, thus lacking an important control activity to reduce risk of inappropriate access and use. Formal policies and procedures would reduce risk by developing an organized monitoring system to track user access and transaction information as well as appropriateness of entitlement provisions. Without formal policies and procedures for monitoring user accounts and activity, the County will remain at risk of inappropriate use; leading to unreliable financial data and human relations security risks.

Specifically we found:

- Operations are managed without formal written policies and procedures, and
- User monitoring is not directed as part of an overall control activity.

Shared Services managers have indicated a willingness to implement the recommendations. The plan is included in this Executive Summary.

For more information regarding this report, please contract Richard Edwards at 919.560.0042 or rcedwards@durhamcountync.gov.

Durham County Government

To: Richard Edwards, Durham County Audit Department
From: Barbara Torian, SAP Shared Services Department Director
Date: May 21, 2010
Subject: SAP Shared Services 2010 Audit Response

Mr. Edwards,

Thank you for taking the time to discuss your audit findings and recommendations with us. As requested, we have formulated and attached our response to your audit points. Please feel free to contact me directly, should you have any questions.

Barbara Torian

Barbara Torian
Director, SAP Shared Services

SAP Shared Services Response

SAP Shared Services fully supports the recommendations of the Durham County Audit Department arising from the audit of SAP system access management. Furthermore, we will begin to take immediate steps towards ensuring all audit points are resolved in as timely a manner as possible within existing constraints. We are steadfastly committed to addressing these recommendations.

Action Plan

SAP Shared Services is proposing the following actions to address the audit points.

Audit Point	**Proposed Action**	**Est. Completion**
Develop formal policies and procedures to provide guidance to SAP Subject Matter Experts (SMEs) and departmental users to monitor entitlement and permission appropriateness.	Create and publish formal policies regarding common scenarios SMEs and departmental users face including but not limited to: • How to review current entitlements. • How to communicate entitlement changes to other SMEs to ensure new entitlements are appropriate for their position. • Investigate a systematic solution to automatically communicate an employee's position change to facilitate prompt correction of entitlements. • Develop a "who does what when" template to ensure each affected party is aware of their responsibilities for maintaining proper entitlements.	12/2010
Provide instructions for handling segregation of duty conflicts in formal policy and procedures documents.	• Publish written instructions to walk department users and SMEs through review and confirmation of employee entitlements. This task would be performed on a periodic basis of no less than 6 months and no greater than 18 months. • Work with SMEs to identify scenarios which comprise violation of segregation of duties. • Require Department Heads to provide written or electronic confirmation identifying by name, users whom they authorize to have entitlements that could be deemed to be in conflict with segregation of duty responsibilities.	12/2010
Develop and communicate to users a system for monitoring user accounts.	There currently exists such an in house system to communicate changes to user accounts. However, while written documentation exists explaining how SMEs are to use it, there is no supporting county policy mandating its use. That policy will be written and proposed for adoption.	3/2011
Develop a system to track compliance with policies and procedures.	Develop specifications for a tracking system to identify those departments in and out of compliance with policies.	6/2011

Dependencies

The ability to successfully implement the above proposed actions are dependent upon the following:

- The issuance of a formal, directive by the County Manager, granting SAP Shared Services the authority to act as the lead SAP user administrator, as recommended by the Durham County auditors.

- Availability of SAP Shared Services technical personnel to complete any systematic changes to enable and promote monitoring, tracking and reporting of changes in user responsibilities that require modifications of entitlements;

- Availability of departmental SMEs to participate in all phases of the effort to monitor, track and report entitlement changes.

***************************************End of Document***********************************

C O U N T Y   O F   D U R H A M

RICHARD EDWARDS
Audit Director
rcedwards@durhamcountync.gov

Internal Audit Department
200 E. Main Street, 4th Floor
Durham, NC 27701
(919) 560-0042
FAX: (919)560-0057

AUDIT COMMITTEE

May 21, 2010

Michael M. Ruffin, County Manager:

This audit of SAP Identification and Access Management was conducted in accordance with the fiscal year 2010 Audit Plan. It was conducted between February 12, 2010 and May 7, 2010.

The audit identified several weaknesses that put the County at risk of unreliable financial and human resource data and information. These risks result from the lack of an orchestrated effort including policies and procedures for users that clearly define responsibilities for monitoring user access and operations within the SAP application.

SAP Shared Services' managers reviewed the report and agreed with the findings and recommendations. They agreed to implement the recommendations by taking the lead on developing policies and procedures and monitoring compliance with them. Shared Services' implementation plan is included in the executive summary of this report.

I appreciate the courtesy and cooperation provided by all the departments and SAP Shared Services' staff.

Richard C. Edwards

Richard Edwards
Audit Director

SAP Identity and Access Management

Table of Contents

Introduction 8

Background 8

Objectives 10

Scope and Methodology 11

Findings and Conclusions 12

IAM Operates Without Official Policy or Procedures 12

Monitoring Of User Activity and Access Needs Improvement 13

Entitlement Monitoring Needs Tighter Controls. 13

SAP User Activity Controls Needs Enhancement. 14

Segregation of duties issues has not been formally addressed. 14

Conclusions and Recommendations 15

Introduction

This performance audit of SAP's Identity and Access Management (IAM) provisions was conducted pursuant to the September 12, 2005 Audit Department Charter which establishes the Audit Oversight Committee and Audit Department and outlines the internal auditor's primary duties. The Audit Committee authorized this audit in July 2009.

A performance audit is an engagement that provides assurance or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria, such as specific requirements, measures, or defined business practices. Performance audits provide objective analysis so that management and those charged with governance and oversight can use the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.[1]

Background

The County's financial and business information is managed via SAP, the County's Enterprise Resource Planning (ERP) system. ERP is an integrated computer-based system used to manage internal and external resources including tangible assets, financial, and human resources. It is a software architecture whose purpose is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders. Built on a centralized database, ERP systems consolidate all business operations into a uniform and enterprise wide system environment. SAP impacts County operations in a number of ways. For example, it is used for financial accounting and payments, contract processing, budget monitoring, human resources and payroll, inventory management, and other functions. Both people and machines are part of the SAP system.

SAP represents a significant investment by the County. It was implemented in October 2005, at a cost of approximately $ 4.5M. SAP business process functions are managed by SAP Shared Services while the hardware, operating systems, and technical tools are managed by the IT department.

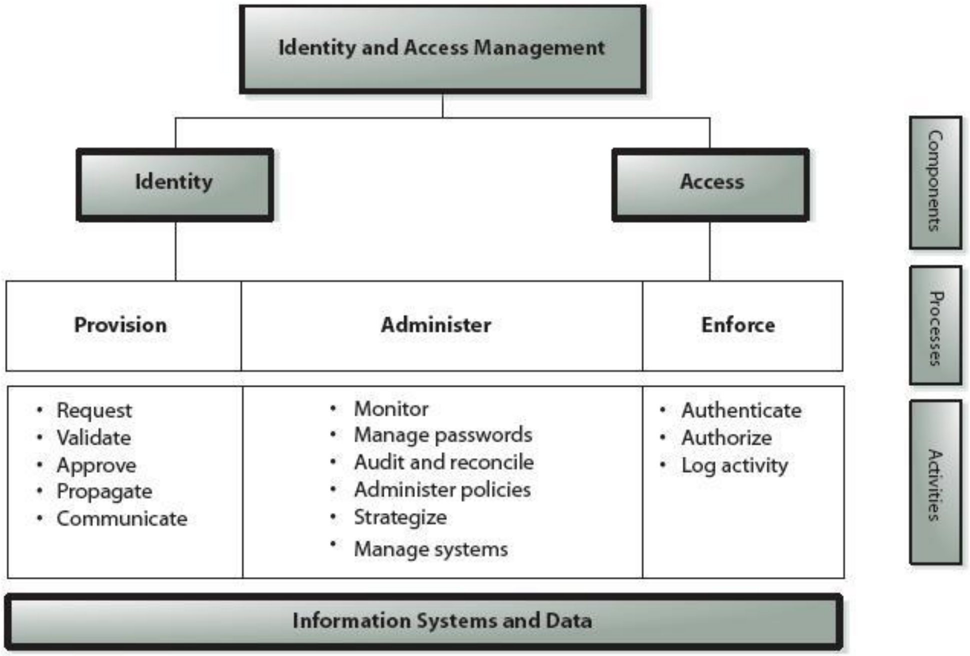
Identity and Access Management (IAM) processes are used to initiate, capture, record, and manage user identities and related access permissions to the organization's proprietary information. It is the process of managing who has access to what business information by creating distinct identities for individuals and systems and the association of system and application-level accounts to these identities.[2] IAM applies to all users, extending beyond County employees. For example, users include

[1] Comptroller General of the United States, *Government Auditing Standards*, Washington D.C: U.S. Governmental Accountability Office, 2007, p. 17

[2] Global Technology Audit Guide, *Identity and Access Management,* Institute of Internal Auditors, p.1

vendors, machines, and generic administrative accounts. Figure 1 provides an overview of the components, process, and activities for IAM.

Figure 1
Identity and Access Management Overview



Source: GTAG Audit Guide P.5

A formal IAM process is not required to attain reasonable security for IT systems, nor is a formal IAM system recommended as a best practice. However, aspects of IAM should be included in system security procedures and processes and should be regularly monitored to ensure the integrity of the information and processes. Specific benefits of IAM include:

- Improved regulatory compliance,
- Reduced information security risks,
- Reduced IT operating and development costs,
- Improved operating efficiencies and transparency,
- Improved user satisfaction, and
- Increased effectiveness of key business initiatives,

The County’s IAM process consists primarily of identification and provisioning. Those are processes to get employees on and off the system. This includes procedures for;

- Identification – the process by which each individual is provided a unique identifier.
- Passwords - a unique code attached to the user identification that allows entry into the network or SAP.
- Entitlements - the permissions to access modules within SAP that enable one to conduct business transactions.

Provisioning is a collaborative effort involving HR, IT, SAP, and operating departments. The initial step is HR's notification to IT that an employee has been hired. HR provides IT with a name and employee number. IT uses that information to create identification (ID); generally the first name initials and surname. That ID is used to access the network as well as SAP unless someone requests an ID expressly for SAP or the user is an individual outside County administration such a Sheriff's Office employee.

After an ID is created, a password is required. IT manages passwords for the network while SAP Shared Services manage passwords for SAP access. Passwords are unique codes created by the employee and can be a combination of alphanumeric characters. Once the password has been created, one can be granted entitlements.

Entitlements are the access privileges one has to use SAP information modules. Entitlements, both initial and as the result of job changes, are granted through a process whereby department managers and supervisors request access directly through the SAP Help Desk or through an intermediary called a Subject Matter Expert (SME). SMEs have the authority to review requests and approve or disapprove them. They make entitlement decisions based upon their knowledge of job roles and the modules for which entitlement is requested. They acquire this knowledge by working in their assigned areas of expertise. For example, the SME in budget is familiar with all the budget modules and can readily determine if an entitlement request from a department outside the Budget Department is appropriate for tasks at the requestor's level.

The County has 15 SMEs stationed in the key business departments; Budget, Finance, and Human Resources. Three of them act as liaisons between SAP and departmental users while the others act as advisors to the three. SAP users in the remaining departments conduct tasks that fall under the umbrella of one of the above three departments.

De-provisioning involves several departments as well. The de-provisioning process design is for HR to send a notice via email to IT to provide employment status information. IT uses the information to cancel the former employee's network password and ID, therefore denying access to the network or SAP.

Objectives

This audit was conducted to answer these specific objective questions:

1. If access authorization methods are appropriate to assure that only those needing access are granted access,
2. Who has access to specific SAP information and is the access authorization justifiable for the task, and
3. Is access and activity monitored, logged, and reported in according with best practices?

Scope and Methodology

Fieldwork was conducted February 12, 2010 through April 23, 2010. We used the Institute of Internal Auditors' "Global Technology Audit Guide - Identity and Access Management" (GTAG) as best practices guidelines for this audit. This guide communicates best practices to address security concerns, and control objectives for effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information and business processes. The institute recommends structure through policies and procedures and regular monitoring of access. Using guidance from GTAG we:

- Interviewed users, administrators, and system managers to identify and obtain information regarding the County's IAM procedures and processes.
- Interviewed administrators and users to obtain information regarding whether entitlement permissions are appropriate for specific jobs.
- Reviewed the IAM procedures and processes to determine if best practices are employed in IAM.

Findings and Conclusions

The County's IAM process is informal, as defined by associations that develop IAM best practices, although several aspects of a formal program are present. IAM efforts operate without the benefit of formal policies and procedures and a single entity has not been designated to act as the focal point to assure that user activity and entitlement permissions are appropriate. SAP Shared Services is best situated to take on the responsibility of guiding the IAM process and we recommend throughout the report that they assume the responsibility. Because the SAP function does not operate according to best practices that encourage controls through written policies and procedures that emphasize monitoring, we recommend that SAP be designated by the County Manager to assume responsibility to:

1. Develop formal policies to provide guidance to SMEs and departmental users regarding entitlement monitoring.
2. Develop and communicate to users a system for monitoring user accounts.
3. Develop a system to track user compliance with policies and procedures.
4. Provide instructions for handling segregation of duty conflicts in formal policy and procedures documents.

IAM Operates Without Official Policy or Procedures

Durham County's IAM processes are conducted without official written policies or procedures. Best practices suggest that policies and procedures be written and communicated to affected parties to enhance controls.

Control activities are the policies, procedures, and practices put into place to ensure that business objectives are achieved and risk mitigation strategies are carried out. Control activities are developed to specifically address each control objective to mitigate the risks identified by management.[3] Policies and procedures assist in four areas of management. The areas are:

- Operations – ensures that fundamental organizational processes are performed in a consistent way that meets the organization's needs,
- Risk management – a control activity needed to manage risk,
- Continuous improvement – improves processes by implementing a Plan-Do-Check-Act (PDCA)[4] approach, and
- Compliance – processes and records that demonstrate effective internal control system compliance with standards, regulations, or laws.

Currently, the County has not designated a controlling authority for SAP or IAM. SAP Shared Services has acted as a facilitator and service provider for the County's use of the SAP application. It provides tools for use by SMEs and departments but without the

[3] IT Control Objectives for Sarbanes-Oxley, ISACA

[4] PDCA is an iterative four-step problem-solving process typically used in business process improvement. Planning is operational goals and direction; Doing is carrying out the plan; Checking is reviewing the data in relation to goals and objectives; and Acting is making changes in the process of procedures that improve effectiveness or altering objectives to be more realistic or meaningful.

authority to direct department managers to monitor users and entitlement permission appropriateness. This role, although useful, does not provide the framework for meeting the above objectives. An entity is needed with authority to develop formal policies and procedures and direct that they be implemented.

Monitoring Of User Activity and Access Needs Improvement

Monitoring is a process to determine if (1) inappropriate access permissions are granted and held, (2) transactions beyond the entitlement's access permissions are conducted, and (3) entitlements pile up over time allowing inappropriate access permissions. The occurrence of any of these conditions is an unacceptable risk to the integrity of system information.

IAM best practices state that "as part of the IAM process, entitlement management should be designed to initiate, modify, track, record, and terminate entitlements or access permissions assigned to user accounts. It further states that the organization should conduct periodic reviews of access rights to detect situations in which users accumulate entitlements as they move within the organization or where users are assigned improper entitlements."[5] These best practices are not carried out consistently leaving the county at risk for security violations through unauthorized and inappropriate use of the SAP system.

The SMEs we talked to were aware of SAP security risks and said they occasionally review entitlements for appropriateness; however, the reviews are not formally structured and included as formal policy or procedures. There is no guidance on steps to take to determine if role definitions are appropriate, if entitlements are appropriate over time, or if users have conducted transactions for which they were not be allowed.

Entitlement Monitoring Needs Tighter Controls.

This report recommends that SAP Shared Services assume the responsibility for providing guidance over SAP related business practices. In that responsibility, SAP Shared Services should provide guidance to departmental users and SMEs on procedures to monitor the appropriateness of entitlement permissions. Currently, as entitlement permissions are granted, they are added to the record and maintained in SAP files. These files can be readily available for review. However, that information is not reviewed to determine if the permissions remain appropriate. Other than at the time of initial entry into the SAP system, it is not known by SAP administrators whether access is justifiable for the employee's task.

Initial provisioning processes assure that the entitlement is appropriate. However, that may not hold true over time as the employee's duties change or as employees move from position to position. When an employee's duties change, their entitlements should be reconciled to the new job. Currently when duties change, the employee or supervisor asks either the SME or SAP Help Desk for access necessary to complete the job assignment. The SME will approve the entitlement if he/she feels the entitlement is appropriate. However, a consistent review process to reasonably assure (1) employees do not amass entitlements

[5] GTAG Audit Guide, p6

and (2) entitlements are appropriate and that segregation of duties issues are known and addressed is not in place.

For such a review process to work effectively, all Durham County operating departments would have to become involved in the process. Each department, working with SMEs would need to review entitlement needs to assure they are appropriate for individual job responsibilities, and forward any adjustments to SAP Shared Services. Currently, there is no consistent effort to do this, as best practices suggest, therefore, risks associated with inappropriate entitlements are high. We recommend that SAP develop a systematic monitoring system and include it in its policies and procedures.

SAP User Activity Controls Needs Enhancement.

According to best practices, SAP activity should be monitored, logged, and reported as necessary. These are internal control efforts to detect and correct risks associated with inappropriate use. The County has the capability through SAP software to conduct these control activities and, in fact, obtains and retains information necessary for monitoring. However, there is no formal process in place to monitor activity, a situation that allows for the risk of unauthorized and inappropriate usage.

We reviewed a sample of 30 employees to determine if they attempted unauthorized transactions. We identified 23 that had made such attempts. We were provided with a method to confirm whether the transactions were completed but decided against it because the results would not have been meaningful over time. We decided that the better course of action would be to point out that transaction monitoring should be used to periodically assure that user activity is appropriate. Monitoring user transactions is suggested by GTAG best practices to determine the risk associated with inappropriate transactions and develop effective control activity.

SAP has the capability to detect and record attempts by employees and the information is available to check if these transactions are beyond the entitlement permissions. SAP also has the capability to determine if such transactions were successfully completed. We recommend that SAP Shared Services periodically sample such transaction attempts as part of its regular monitoring program. Over time, an accumulation of data and analysis will provide a baseline to determine the need for future testing to acquire the level of assurance that the internal system controls are adequate.

Segregation of duties issues has not been formally addressed.

The lack of segregation of duties is an issue in the County's SAP operations. Of the 30 cases we reviewed we found that six of them were given entitlements that had segregation of duties issues. For example, entitlements that granted the permission to create a purchase order also permitted receiving. Such a condition is considered risky, calling for mitigation under ordinary circumstances. During discussions with an SAP administrator, the condition was acknowledged; however, a remedy to the condition is not apparent. For example, in departments with limited staff resources, segregation of duties may not be possible, and other ways of mitigating the risk need to be explored.

Conclusions and Recommendations

The County's SAP operation has processes that meet best practices. However, there are voids that should be filled to provide a greater level of system security and decrease overall risk. The lack of (1) formal policy and procedures and (2) a formal monitoring program, leaves the County at risk of inappropriate or unreliable financial and HR activity or data. Best practices encourage mitigation of those risks by control activities that provide assurance over time that the SAP operation is providing benefits for which it was designed and implemented. To achieve these objectives we recommend that upon designation by the County Manager SAP Shared Services:

1. Develop formal policies and procedures to provide guidance to SAP Subject Matter Experts (SMEs) and departmental users to monitor entitlement permission appropriateness.
2. Develop and communicate to users a system for monitoring user accounts.
3. Develop a system to track compliance with policies and procedures.
4. Provide instructions for handling segregation of duty conflicts in formal policy and procedures documents.