Countywide User Access

May 27, 2016

A Report to the Jackson County Board of Commissioners

Commissioners

Doug Breidenthal

Rick Dyer

Colleen Roberts

County Administrator

Danny Jordan

Internal Audit Program

Eric Spivak
County Auditor

Tanya Baize
Senior Auditor

Nicole Rollins
Senior Auditor

JACKSON COUNTY
Oregon

MEMO
INTER-OFFICE

Internal Audit

Eric Spivak
County Auditor

10 S. Oakdale, Room 214
Medford, OR 97501
Phone: (541) 774-6021
Fax: (541) 774-6705
SpivakER@jacksoncounty.org

To: **Board of Commissioners**
Re: **Audit of Countywide User Access**
Date: **May 27, 2016**

The enclosed report presents the results of our audit of user access of the County's computer network and the financial and human resources system (EnterpriseOne aka E1).

The objective of the audit was to evaluate the design and implementation of controls regarding:

1) The granting of and removal of access to the network and systems
2) The appropriateness of access levels granted, given each employees job duties and functions
3) The segregation of duties and/or use of mitigating controls to offset risks that arise when access levels grant a user access to multiple areas of a system

We found that controls have been designed and implemented which conform to industry best standards. These controls provide an appropriate level of control over user access to EnterpriseOne (E1) and the County network. We did not make any recommendations within our report.

We worked closely with the IT department on this audit. During our discussions, it was agreed that there is a risk of individuals placing sensitive or confidential information in unsecure network locations. IT will purchase software that can be used in an attempt to identify sensitive information placed in unsecure locations.

Please feel free to contact me at your convenience if you have any questions or would like additional information not contained in the report.

C: Audit Committee
Moss Adams, LLP

Audit Results

Why We Did This Audit

We conducted this audit in accordance with the FY 15-16 Internal Audit Plan.

Our objectives were to determine if controls have been designed and implemented that:

-Restrict access to appropriate individuals

-Grant access based on need to perform job

- Provide for appropriate segregation of duties or mitigating controls

What We Recommend

We did not make any recommendations. Per discussion of inherent system risks with the IT department, IT will be purchasing software that can be used in an attempt to identify if sensitive information has been placed in inappropriate network locations.

JACKSON COUNTY
Oregon

Countywide User Access

What We Found

Controls have been designed and implemented which conform to industry best standards and provides an appropriate level of control over user access for EnterpriseOne (E1) and the County network.

Introduction & Background – Countywide User Access Audit

Introduction and Background

The Information Technology (IT) Program develops and maintains the computer information systems and communication networks which County employees depend on to serve the community and internal customers. This includes supporting a wide variety of software applications, such as the County's financial and human resources system referred to as EnterpriseOne (E1). IT is considered a central service program, as such the majority of the funding for the program comes from other County departments.

The IT Program has 29 FTE in the fiscal year 2015-16 adopted budget, which accounts for approximately 60% of the $5,527,696 IT budget. The remaining 40% of the budget is made up of materials and services and capital outlay.

E1

The County went live on July 1, 2004 with the financial module of the E1 software system. Other modules followed, which allowed the integration of financial, payroll, budget and human resource into one system.

With the different functionalities of the software, access to the software system needs to be appropriately assigned and limited. There are 45 user roles. Each user role limits the user's ability to perform certain functions within E1, such as accounts payable or budget related tasks. There are approximately 673 active E1 users.

Network

Network access provides the means to maintain computer security and the ability to limit access to things such as internet and data storage locations. There are approximately 848 network accounts.

Audit Authority

We conducted our audit in accordance with Codified Ordinance 218 pertaining to the County Auditor. Our audit was included in the fiscal year 2015-16 Internal Audit Plan.

Compliance with Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. These 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.

Confidential or Sensitive Information

All systems have vulnerability risks. We reviewed these risks associated with user access and the compensating controls used to mitigate these risks. We did not include this information in the report but we did discuss the information with appropriate management personnel and the Audit Committee.

Audit Objectives

The objectives of the audit were to determine if:

1. Only active employees have access to E1 and the network.
2. Rights and permissions were directly aligned with the employees' position duties and responsibilities.
3. If segregation of duties or mitigating controls provided adequate control against the risk of errors or fraud occurring.
4. An appropriate employee performs the review of user account rights and permissions.
5. Privileged or elevated access is limited to only those employees with a proven need for that access.

Audit Conclusion

Controls have been designed and implemented which conform to industry best standards and provide an appropriate level of control.

Audit Scope and Methodology

This audit included all County departments. The audit focused on reviewing current practices used to grant and revoke user access.

Audit procedures included:

- Interviewing key department personnel.
- Reviewing lists of each department's employees that have the authority to grant and revoke access.
- Reviewing bi-annual E1 user access role reports and monthly network reports.
- Reviewing user role assignments for appropriateness based on job position and function.
- Verifying that appropriate documentation is maintained so that there is a record of when access is granted and when it is revoked.

- Verifying that only active employees have access.

Audit Criteria

Criteria consisted of County policy *Computer and Communications systems Operation and Security*, best practices as established by the U.S. Government Accountability Office (GAO), and best practices as established by the Information Systems Audit and Control Association (ISACA).

Audit Results – Countywide User Access Audit

Only Active Employees Have Access

We found that controls provide adequate assurance that only active employees have access. The primary control is that the user department promptly notifies Information Technology (IT) when an employee is leaving employment with the County so that IT can then revoke the user's access. The secondary control is that on a monthly basis IT sends each department a list of employees and contractors who have not signed-in to the network within the last 30 days. If a department does not confirm with IT that the access is still needed within 7 days, IT disables that user's access.

We performed the following to ensure that controls are adequate:

- **Reviewed a sample of employees that recently separated employment** – We selected a sample of 26 employees from the period of February 2015 through January 2016 and verified that the department contacted IT and that the user's access was revoked in a timely fashion. There was a delay in notifying IT for 2 of the 26 individuals.
- **Reviewed two monthly reports** – We reviewed the monthly reports for November 2015 and December 2015 and verified that there is a process in place to notify departments when users have been inactive for 30 days.

  In reviewing the monthly reports, the results revealed that departments are diligent in notifying IT when employees terminate. However, departments are not as diligent in remembering to notify IT when an extra help employee or contractor completes an assignment and no longer needs access. For example, Internal Audit forgot to notify IT when the external auditors were done with their testing and no longer needed system access.
- **Confirmed that employees who separated employment with the County no longer have access.** We pulled a listing of separated employees and compared that listing to current user accounts. We found all access had been removed for all former employees.

Access is Granted to Employees Based on Request by Department

We found that controls provide adequate assurance that user access is limited. Access is granted only upon request from an authorized representative of the user's department. However, per discussion with IT

there is an inherent risk that sensitive information could be saved to a data storage location that was not intended to house the sensitive information. Therefore, the network access granted to an individual might be appropriate but there is the risk that an individual could access information that shouldn't have been stored in that location.

The primary control is that an appropriate individual at the department sends a request to IT to grant an employee access to specific E1 roles and network access based on that employees' position and job function. IT will grant the access as requested. If the request seems unreasonable based on the employee's position and job function, IT will contact the department to determine what roles are appropriate for that employee and/or to ask for approval from a higher level of authority. The secondary control for E1 access is that on a bi-annual basis IT sends each department a listing of all individuals with E1 access and the roles each user has been granted, such as the accounts payable role. The department is responsible for reviewing the listing for reasonableness and then informing IT of any needed changes.

We performed the following to ensure that controls are adequate:

- **Verified that employees assigned the authority to request access were appropriate.** We found that employees who are designated as the point of contact for user access requests were appropriate.
- **Reviewed who was assigned to each of the E1 user roles for reasonableness.** We pulled a listing of all individuals assigned to each one of the E1 user roles and reviewed the listing for reasonableness based on the individuals' job title and function and the auditor's knowledge of County departments and the functions within each department. We identified that the Internal Audit staff had access that was no longer needed but we did not identify anything else that needed changing.
- **Reviewed a sample of 17 employees that had a recent change in position, department, and/or program within a department to ensure that the E1 roles had been modified as appropriate.** We found that E1 access roles to be appropriate both before and after the change in position, department, and/or program within a department.
- **Reviewed a sample of 10 employees' network access for reasonableness.** We found that the 10 employees sampled had network access that seemed reasonable based on each employees'

position and job function. As touched upon briefly above, access granted to data storage locations restricts the user to a specific location but there is an inherent risk that sensitive information could be saved in a location that is not intended to house that information. For example, someone could save a spreadsheet with sensitive information to a shared folder that can be accessed by the entire department and is intended only for storage of non-sensitive items such as policies, procedures, and forms.

Given this inherent risk, IT has determined that it would be beneficial to purchase a software tool that can be used to identify sensitive information and the location of that information (e.g., the software will search for a string of nine numbers since a nine number string could be a social security number).

Segregation of Duties – E1 User Roles

We found that compensating controls have been designed to mitigate the risks that result when a particular E1 user role provides the ability to perform related tasks. The term "role" is used to describe a grouping of related tasks and a "user" is a person who has been given the role designation and can therefore perform the tasks. For example, the accounts payable user role enables a user to perform related tasks such creating and modifying vendors, creating purchase orders, and processing payments.

Having the ability to perform related tasks increases the risk of errors or misappropriations. Appropriate compensating controls that would prevent and/or detect the occurrence of these risks have been implemented.

The E1 user roles are structured to address specific functions, such as:

- Accounts Payable
- Accounts Receivable
- Budget
- Information Technology
- Employee Processing
- Fix Assets
- General Accounting
- Human Resources
- Payroll
- Supervisor
- Time Entry

We discussed some of these functions with appropriate personnel to gain an understanding of what access each user role permits and what compensating controls are in place to prevent error or malicious intent.

The user role weaknesses and compensating controls were not included in this report since the information is considered sensitive. The weaknesses are known by the appropriate managers and compensating controls have been instilled within E1 or through manual processes.

Periodic Review of E1 User Access is Occurring

We found that a control has been designed and implemented to provide the departments with a mechanism to periodically review E1 user access roles for the purpose of ensuring that employees' access is still appropriate. As mentioned earlier, there are bi-annual E1 user role reports for departments to review to determine if each individuals' E1 roles are appropriate given the employees' position. There is no similar control for network access. Producing a report for network would be cumbersome. Also, the risk isn't necessarily the access granted to a specific location, but the information housed within a specific location. As discussed earlier, IT will obtain software to identify locations where sensitive information is being stored to be able to further evaluate this risk.

Privileged or Elevated Access is Limited

We found users with privileged or elevated access are appropriately limited to only those employees with a proven need for that access. We also reviewed user roles that are restricted to specific functions, such as access to change pay information, for reasonableness. We did not identify any concerns.