Performance Audit:

Identity and Access Management

Durham County Internal Audit Department

May 4, 2017

Richard Edwards
Internal Audit Director
rcedwards@dconc.gov

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

Audit Committee:
Manuel Rojas
Arnold Gordon
Harrison Shannon
Wendy Jacobs
James Hill

May 4, 2017

Mr. Wendell Davis,
County Manager

Dear Mr. Davis:

Internal Audit has completed its review of Durham County's Identity and Access Management (IAM) controls regarding information systems and information. The audit focused on internal controls in place to (1) allow only approved personnel the ability to access IS&T systems, (2) terminate timely employees' systems access when they separate from service and (3) assure that employees, including contractors and consultants, do not have access to information and systems beyond what is appropriate for their jobs. We found access terminations were not done timely. Some employees remained in the system for up to 17 days after they were no longer employed. Best practice suggests that access be terminated no later than the day an employee is terminated.

Except for two cases in which promoted employees were given inappropriate roles (manager roles instead of supervisor roles), controls were in place, and operating appropriately to assure that system access was granted according to employees' needs. In these two instances, the employee granting access made both errors on the same day while filling- in for the person that customarily performed tasks associated with granting access.

This report recommends several processes to enhance controls in the above processes. Those recommendations are on page seven of this report. This report's findings and recommendations have been reviewed by the HR Department. Departmental comments, including corrective actions, are included in the report as appendix 1.

The audit work was conducted by Ms. Kierra Simmons and Ms. Alecia Amoo. The audit team appreciates the cooperation and assistance provided by IS&T and HR staff during the engagement.

Sincerely,

Richard C. Edwards

Richard Edwards,
Internal Audit Director

INTRODUCTION

The Audit Oversight Committee approved this audit in the fiscal year 2017 Annual Audit Plan. This audit was conducted in order to identify and examine Identification and Access Management (IAM) controls for Durham County's information systems that include both the Network and the Enterprise Resource Planning system (ERP).

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. I believe the evidence obtained provides a reasonable basis for the findings and conclusions based upon the audit objectives.

Performance audits are defined as audits that provide findings or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using 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

Durham County employs approximately 1900 employees. Additionally, the County uses various contractors and consultants (consultants) as required. Employees and consultants need access to certain County information and communication media to conduct their business. All employees and consultants, except those in remote locations, are given access to the County's "Network" which includes the email system and other programs and operational software such as word processing tools needed to conduct their work.

In addition to the Network, some employees and consultants have access to SAP, the County's Enterprise Resource Planning (ERP) system. This system maintains the County's financial, human resources, and other critical operational information. Access to both the Network and SAP is granted via joint efforts by the Human Resources (HR) Department, Information Systems & Technology (IS&T) Department, and departmental experts. The HR Department is involved through onboarding of employees and consultants, and the IS&T Department provides access through its maintenance of the information systems. Departments and their experts request or direct access as required in performing specific tasks within departments.

IAM is the tool or process for managing who has access to certain information in an organization. It initiates, captures, records, and manages user identities and access permissions to an entity's information. Generally, IAM it is made up of (1) passwords and identification codes, (2) methods to match job descriptions to system access, and (3) a mechanism to provide greater or lesser access as required in cases of promotion

[1] Comptroller General of the United States, *Government Auditing Standards,* Washington D.C.: U.S. Governmental Accountability Office, 2011, p.17.

or job changes. IAM also includes removal of individuals from information systems who are no longer employed or otherwise do not have a legitimate need for access.

The IAM process in Durham County is centralized around the User Access Request (UAR) system, a database used by Human Resources, IS&T, and operating departments to request, process, store, and document user accounts. Using this database, authorized users such as managers and supervisors can initiate requests for granting and terminating users' access to the Network and to SAP.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

This audit was conducted to answer three specific objective questions. They were: (1) is a creditable system in place that identifies persons before they can access IS&T systems (2) is access for separated employees and consultants timely terminated, and (3) are controls functioning in a manner that ensure that County systems and information are accessed only as needed?

To conduct our review, we:

1. Reviewed relevant policies and procedures governing identity and access management.
2. Interviewed IS&T's SAP, Departmental Subject Matter Experts, HR personnel, and Department Supervisors.
3. Tested a sample of 72 users, 42 of which had access to the Network only and 30 with additional authorizations for SAP access. Our review period was April 25, 2016 through September 26, 2016.
4. Researched best practices for identity and access management.
5. Compared best practice concepts with the County's current practices.

FINDINGS AND CONCLUSIONS

Processes for timely removal of Network and SAP access need to be enhanced to meet industry best practices. We found that 40 of 42 terminations we reviewed were not completed by the time the employee separated from employment as recommended by best practices. Although most cases we reviewed were processed later than best practices suggest, we did not identify instances in which access terminations had not been completed.

Additionally, we identified two instances in our sample of 30 cases in which two promoted employees were given supervisory and manager access when they should have only been given supervisory access. We believe the minimal number of errors is due to the skill and attention level of the persons processing the permissions. The process for inputting codes into the system is manual and therefore subject to errors like the two we identified. To provide greater assurance that such errors will be minimal, we recommend that an employee filling in for a regular employee be fully trained.

Processes for granting initial and continued access to IS&T systems through the passwords process were conducted in accordance with best practices. Controls over that process requires appropriate authorization. In addition, IS&T requires employees to update passwords every 90 days as a security measure over who is able to access the systems.

User Termination of Access Need to be Timely

Delays in terminating separated employees from the system is a security risk for the County. This risk can be lessened by more timely terminations of system access for separated employees. Forty of the forty-two separated employees we reviewed were not terminated timely. Terminations ranged from one to 17 days past employee separation dates. During those periods, separated employees could have accessed the County's IS&T systems, although; we did not find evidence that any had done so. Industry best practices suggest access terminations take place no later than the date the employee separates from employment.

To terminate an employee, the manager only has to complete a request form located in the IS&T module located on the computer. This form, once completed, is directly submitted to IS&T. Audit results showed that managers and supervisors take, on average, about five days after the employee separates to notify IS&T that an employee has been separated. It takes another day for IS&T to implement the termination.

Supervisors and HR personnel provided several causes for untimely terminations. Causes included:

1. Miscommunication about who is responsible for initiating a request for termination.
2. Not identifying a back-up employee to request termination when the supervisor is out of the office.
3. HR completing an employee relations review prior to initiating a termination request. (If the employee relations review is delayed due to outstanding performance appraisals or due to the payroll process beginning, then the request for termination will be delayed).

This report recommends that HR develop policies requiring responsible supervisors and managers to initiate action to terminate access no later than the time the employee separates. According to one HR representative, this is possible because most employees provide notices of their separation, many at least two weeks before they separate from service.

Errors are Possible in Granting Access

The access granting process, a function of a network of managers, supervisors, and Subject Matter Experts (SMEs), have controls, but the controls are primarily signatory in nature. For example, access cannot be granted unless someone in authority authorizes it. This authorization is observed through the channels in which requests are routed and specific sign-offs are given. This signatory process controls who is granted access for specific purposes. However, weakness in the controls exist at the point where access codes are entered into the system. The entries are made manually by departmental experts who are familiar with the SAP system and the various roles within the department. The person making the entry selects from a menu of options present in the system and "clicks" on the correct option. There are some internal machine controls in place to notify the entry person when an invalid entry has been made, however; the machine does not control all entries.

Therefore, there are possibilities for errors in the manual entry process. The process relies heavily upon the skills, expertise, and experience of the person entering the access codes.

Internal Audit reviewed the process of granting access and reviewed 30 cases for accuracy. We identified two employees out of 30 that received incorrect user access authorizations. In both instances, the employees changed job positions and were granted access authorizations beyond what was appropriate. Specifically, both employees held supervisor positions and were subsequently promoted into other supervisory positions. During the process of changing access, the SME, or departmental expert, granted access authority reserved for managers in addition to supervisory access. As noted earlier, the system does not have a control mechanism to stop such errors. Based upon discussions with SMEs, Internal Audit believes that the minimal number of errors we identified is due to the skill and experience levels of the persons entering the codes.

The two errors we identified were committed by the same person, each error occurring on the same day. The SME that committed the errors was filling-in temporarily for the regular SME. The relief SME said she made the mistakes because she lacked sufficient training and experience in approving access authorizations. Best practices emphasizes cross training where feasible and Internal Audit recommended cross training as needed. HR agreed with the recommendation and indicated it would emphasize cross training as part of its business practice.

<u>The User Access Request (UAR) System Anchors IAM</u>

The IAM process in Durham County is centralized around the User Access Request (UAR) system, a database used by Human Resources, IS&T, and operating departments to request, process, store, and document user accounts. Using this database, authorized users such as managers and supervisors, can initiate requests for granting and terminating users' access to the Network and to SAP.

The initial process is the granting of identifications and passwords. Passwords are granted when persons are hired and a subsequent request is made by the hiring department to grant a password. HR is the approver of passwords through its on-boarding process. Although a hiring department may complete the UAR, it will not be approved without the appropriate authorization from HR. When proper authorization is granted, IS&T will provide an identification, usually the employee's name, and will allow the employee to select a password.

Password, identification, and sign-in protocols are standard practice for entry into secure systems. Valid identification and passwords along with proper input of this information is necessary to access IS&T systems. Additionally, passwords must be updated every ninety days. Because of these practices, we believe IS&T operates in accordance with industry best practices as it relates to IAM.

RECOMMENDATIONS

To enhance controls regarding the reported findings, we made the following recommendations to the IS&T and HR Departments:

1. Develop policies requiring responsible supervisors and managers to initiate action to terminate access no later than the time the employee separates.
2. Clarify who is responsible for initiating a request for termination.
3. Develop and implement a process to complete employee reviews so access can be terminated at the time of employee separation.
4. Ensure that employees and those who may fill-in for critical employees have appropriate training.

Appendix 1: Departmental Comments

DURHAM COUNTY Human Resources

April 24, 2017

Richard C. Edwards
Internal Audit Director
Durham County Government

Dear Mr. Edwards,

Human Resources is in receipt of your Performance Audit Identification and Access Management for Durham County's Information Systems, wherein you made specific Findings and Recommendations. The report has been reviewed by key members of the Human Resources Leadership Team and at the conclusion of a very thorough examination of the same, it is HR's plan to adopt the recommendations offered in the report in its entirety. Specifically, HR's short-term goals include the implementation of an Offboarding Module for supervisors to initiate the employee separation process before the employee's last day of employment with the County.

Please note the responses listed below regarding your recommendations:

1. Develop policies requiring responsible supervisors and managers to initiate action to terminate access no later than the time the employees separates. ***Response:*** Currently, supervisors and managers are able to lock an employee's access to all networks via the Current Employee Request form on DCInfo. HR and IS&T will ensure the process is communicated to supervisors and managers.
2. Clarify who is responsible for initiating a request for termination. ***Response**:* The department is responsible for submitting the request to lock network access. HR is responsible for ensuring the system access for a separating employee is disabled or deleted via the HCM separation action. HR and IS&T will ensure the process is communicated to supervisors and managers.
3. Develop and implement a process to complete employee reviews so access can be terminated at the time of employee separation. ***Response:*** HR will continue to work with departments to ensure all performance appraisals are received in a timely manner.
4. Ensure that employees and those who may fill-in for critical employees have appropriate training. ***Response:*** HR has discussed role assignments with the appropriate employee and clarified all misunderstandings.

Thank you for this opportunity to respond. If you have any questions regarding this response, please feel free to contact me.

With kind regards, I am

Sincerely,

Kathy R. Everett-Perry, Esq.
Chief Human Resources Officer - Director