Performance Audit:

SAP Identity and Access Management

Durham County Internal Audit

January 17, 2025

Richard Edwards
Internal Audit Director
ricedwards@dconc.gov

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

January 17, 2025

Claudia Hager, County Manager:

Internal Audit has completed its review of the County's SAP Identity and Access Management. This audit was conducted in accordance with the Audit Department's Charter, dated September 12, 2005, and aligned with Generally Accepted Government Auditing Standards (GAGAS).

As outlined in the report, this performance audit was conducted to evaluate the County's controls for employees using the Enterprise Resource Management System (SAP). Our objective was to determine if authorization methods were appropriate to ensure that only those needing access were granted access and if access authorization levels were appropriate for assigned tasks and job duties. The scope of the audit included only those employees who had the ability to create or approve financial transactions within SAP. Our audit was conducted from August 2024 through November 2024.

We did not identify instances in which Identity and Access controls were not working properly in our audit. Authorization controls and access levels within SAP were commensurate with assigned tasks and job duties.

We did not make any recommendations as this audit did not identify any negative findings. Thank you for you and your team's cooperation during the conducting of this audit. We would like to express our gratitude to IS&T and their team for their cooperation throughout this process.

Sincerely,

Richard Edwards

Richard Edwards

Internal Audit Director

CONTENTS

INTRODUCTION

This audit of SAP Identity and Access Management was conducted pursuant to the September 12, 2005, Audit Department Charter which establishes the Audit Oversight Committee and the Audit Department and outlines the internal auditor's primary duties.

Performance audits provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight with, among other things, improving program performance and operations, reducing costs, facilitating decision-making by parties responsible for overseeing or initiating corrective action, and contributing to public accountability.[1]

AUDIT OBJECTIVE

We conducted this audit to review Durham County's controls for employees using the County's Enterprise Resource Management System (ERP). Without adequate controls, the County is at risk for fraud, waste, and abuse. The County's ERP system is commonly known as SAP.

Our focus was on employees in positions whereby they can make financial entries and approvals in the general ledger. For employees who had or have such roles, we asked the following questions:

1. Are authorization methods appropriate to ensure that only those needing access are granted access?
2. Are access authorization levels appropriate for assigned tasks and job duties?

BACKGROUND

The County has used SAP as its ERP system for approximately 19 years. It is the tool employees use to conduct operations such as Payroll, Budgeting, Purchasing, Human Resources, and other functions. As such, SAP's financial modules are essential for processing, approving, and recording the County's financial transactions.

All employees in the County have access to at least one SAP module, with some having access to several modules. For example, this access ranges from the

[1] Comptroller General of the United States, *Government Auditing Standards,* Washington D.C: U.S. Governmental Accountability Office, 2024, p.11

employee who has minimal access and can review his or her pay records and enter working hours. Other employees may require more complex access because their job duties require them to process pay and subsequent pay records.

The critical and various uses of SAP require a system that is accessible for users while having mechanisms in place that provide security for the County's financial and personnel data. At a minimum, security processes should assure that access is granted commiserate to an individual's need or job duties.

SAP security for financial data, our focus in this audit engagement, begins with the job assignment. Along with authorizing access as required, security measures extend to assuring that authorizations are withdrawn once they are no longer appropriate.

SCOPE AND METHODOLOGY

This performance audit was conducted following Generally Accepted Government Auditing Standards (GAGAS). These standards require that we plan and execute the audit in a manner that ensures sufficient, appropriate evidence is obtained to provide a reasonable basis for the audit's findings and conclusions, in alignment with the stated audit objectives. The evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

The fieldwork was conducted from August 2024 through November 2024, and covered new hires, employees with additional roles, employees with reduced roles, and removal of employees from SAP because they are no longer employed. This included all 187 employes who had access to enter or approve financial transactions, during the above period. Our methodology included:

A. reviewing formal policies about user management,
B. examining user access records,
C. reviewing user roles within SAP's financial modules,
D. identifying departmental authorization workflows, procedures, and policies,
E. interviewing key personnel involved in financial transactions, including.
    1. finance managers,
    2. subject matter experts,
    3. system administrators,
    4. various end-users, and
    5. departmental heads responsible for overseeing transaction authorizations.

WHAT WE FOUND

The controls in place for the 78 User Access Requests (UARs) and 187 employee access records we reviewed were within the level of controls established by the County and industry best practices. Below is a summary of review results for the audit objectives for the audit engagement.

Authorization Controls Were Appropriate

User Access Requests is the method or system by which employees are granted access to use the County's information systems. User access requests are generally initiated by the employee's direct supervisor, or a designated employee from the Human Resources (HR) Department. For the 78 UARs we reviewed, authorization methods were appropriate to ensure that only those needing access were granted access. These UAR requests included onboarding requests for new hires, requests to add or remove specific roles for users, and contractor additions or changes.

User access requests were properly submitted by the appropriate parties based on what their job duties are and the functions they would need to perform within SAP. In instances where requested roles were not common for the position, or if requested roles appeared unnecessary, requests were properly sent to those who understand which roles are necessary for specific job functions. Such employees are referred to as Subject Matter Experts (SMEs). Once SME's received requests, they either appropriately approved or denied role changes, based upon their understanding of the employee's needs for their position.

Authorization methods were appropriate.

Authorization Levels Were Appropriate for Assigned Tasks and Job Duties

For the 187 records we reviewed, access was appropriate for assigned tasks and job duties. Segregation of duties, whereby an employee could have the ability to make several entries that would allow the potential to breech controls were not evident in the cases we reviewed. Additionally, to strengthen security, SAP has a built-in mechanism that prevents an employee from completing multiple steps of an entry, ensuring that no single employee has end-to-end control over any financial process. The system itself ensures that one employee cannot both initiate and approve the same transaction.

Access was appropriate for job duties.

We also found that IS&T initiates an entitlement review, at least once a year, to review current levels of roles for users within SAP. These entitlement reviews are directed at the Subject Matter Experts for HR, Budget, and Finance. We found

that in some instances, the SMEs will generate a review themselves and submit requests to IS&T to make the necessary changes to employee roles. These reviews are done to ensure access that is no longer necessary is removed, based on the current employee positions and the needs of each position.

CONCLUSION

We believe the security systems for Durham County's IAM controls are adequate to reasonably assure that only those that need access to SAP are granted access, and the access is only what is necessary for their job duties.

RECOMMENDATIONS

This report did not identify negative findings. Therefore, Internal Audit did not make specific recommendations.

APPENDIX I

Information Services & Technology

TO: Richard Edwards, Durham County Internal Audit Department

FROM: Greg Marrow, Information Services and Technology Department

DATE: January 17, 2025

SUBJECT: SAP Identity and Access Management Audit 2025

Mr. Edwards,

Thank you and your team for providing the report for the SAP Identity and Access Management Audit. After our review, we agree with the report having no negative findings. If any additional information is required, feel free to contact me.

DocuSigned by:
Greg Marrow
625C0D2677AD493...
Greg Marrow

Director, Information Service and Technology

200 E. Main Street, Durham NC 27701