Mecklenburg County
Department of Internal Audit

Human Resources
PeopleSoft Application Security Follow-Up Audit
Report 2208

September 16, 2022

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency and good governance.
Internal Audit Contacts	Terry Thompson, CIA, CRMA, Audit Director (980) 314-2889 or terry.thompson@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2893 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Robert Nebel, CIA, CISA, Auditor-in-Charge
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at https://www.mecknc.gov/audit/reports/pages/default.aspx?

MECKLENBURG COUNTY
Department of Internal Audit

To: Dena Diorio, County Manager
County Manager's Office

From: Terry Thompson, Director
Department of Internal Audit

Date: September 16, 2022

Subject: Human Resources PeopleSoft Application Security Follow-Up Audit Report 2208

The Department of Internal Audit completed a follow-up audit on reported issues from the PeopleSoft Application Security Audit Report 1452 issued February 9, 2015. The follow-up audit objective was to determine with reasonable but not absolute assurance whether management took effective corrective action on the issues presented in the audit report.

Internal Audit staff interviewed key personnel, observed operations, reviewed written policies, procedures, and other documents, and tested specific transactions where applicable. Internal Audit conducted this audit in conformance with The Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing.

FOLLOW-UP SUMMARY

There were eleven recommendations in the PeopleSoft Application Security Audit Report 1452. The following table provides the original number of recommendations and summarizes the follow-up audit results performed to date.

Fiscal Year	Audit Report	Implemented	Open	Not Implemented[1]	Withdrawn	Total Carryforward
2015	1452[2]	N/A				11
2015	1585	5	6			6
2018	1815	1	5			5
2019	1917		5			5
2022	2208	2	3			3

[1] Management assuming risk for not taking corrective action
[2] Initial report

Details regarding the most recent follow-up audit are noted in the attached **Follow-Up Results** matrix. Internal Audit will review any carryforward issues later to verify recommendations are fully implemented and working as intended. Recommendations considered implemented will be excluded from further review.

The cooperation and assistance of the Human Resources staff are recognized and appreciated.

c: Assistant County Managers
County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee
Director, Human Resources

Follow-Up Results
PeopleSoft Application Security Audit Report 1452

- **Implemented –** Audit issue has been adequately addressed by implementing the original or alternative corrective action plan **(I)**
- **Open –** Corrective action for audit issue initiated but not completed **(P)**; Implemented but not operating as intended **(IO)**; Not been addressed but management fully intends to address issue **(O)**
- **Not Implemented** – Audit issue not addressed and management has assumed the risk of not taking corrective action **(NI)**
- **Withdrawn** – Audit issue no longer exist due to operational changes **(W)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
1.1	Internal Audit recommends management develop and implement formal PeopleSoft operational policies, procedures and standards for: • Application security risk assessments, including identification of high risk business processes and transactions • Development of security roles, including ongoing security role maintenance • User access controls, to include but not be limited to, user identification and authorization; user identifications (User ID) and password management; system delivered User IDs; sensitive accounts and related privileges; and other sensitive application resources • System security monitoring and auditing activities • Configuration management, including purpose, scope, roles, responsibilities, baseline configuration, management commitment, coordination among relevant entities, compliance, and implementation	HRMS, IT Applications & Database and Finance-Payroll will partner to develop policies and procedures that will ensure a consistent method of administering application security management, monitoring, auditing and a continuity plan.	03/2015	P	Internal Audit determined procedures for business continuity have been formally developed and implemented. However, procedures for application security risk assessment were under development and not complete. Management indicated the recommendation is partially implemented due competing priorities and changes in staff and department management.

Follow-Up Results
PeopleSoft Application Security Audit Report 1452

- **Implemented –** Audit issue has been adequately addressed by implementing the original or alternative corrective action plan **(I)**
- **Open –** Corrective action for audit issue initiated but not completed **(P)**; Implemented but not operating as intended **(IO)**; Not been addressed but management fully intends to address issue **(O)**
- **Not Implemented** – Audit issue not addressed and management has assumed the risk of not taking corrective action **(NI)**
- **Withdrawn** – Audit issue no longer exist due to operational changes **(W)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
	of the policy and associated controls • Business continuity planning, including development, implementation, and testing				
3.1	Internal Audit recommends management work with IT and review role assignments for PeopleSoft programmers, and place appropriate restrictions on their access to production and development environments. In addition, management should work with IT to create a formal, documented segregation of duties framework for system security access and periodic monitoring.	IT will review role assignments for PeopleSoft programmers, and place appropriate restrictions in the production environment to remove the potential for programmers to inadvertently, or purposely, change production data. We do exercise more flexibility for programmers in the development environments as this expedites testing, enabling the programmers to see the full function of changes without actually updating the production system. There is no risk to production from these operations in the development environment. This will be completed by first quarter 2015. In addition, management and IT will work to create a formal, documented segregation of duties framework for system security access and periodic monitoring. This will be completed by first quarter 2015.	03/2015	I (1) IO (1)	Internal Audit determined a review of role assignments for PeopleSoft programmers was performed and a separation of duties (SOD) framework was developed. However, the SOD framework was not aligned with current roles and activities performed within PeopleSoft.
4.1	Internal Audit recommends management define and implement	HRMS, Finance and IT will define how to move forward with auditing and	03/2015	O	Management indicated the recommendation is open due competing priorities and changes in staff and

Follow-Up Results
PeopleSoft Application Security Audit Report 1452

- **Implemented –** Audit issue has been adequately addressed by implementing the original or alternative corrective action plan **(I)**
- **Open –** Corrective action for audit issue initiated but not completed **(P)**; Implemented but not operating as intended **(IO)**; Not been addressed but management fully intends to address issue **(O)**
- **Not Implemented** – Audit issue not addressed and management has assumed the risk of not taking corrective action **(NI)**
- **Withdrawn** – Audit issue no longer exist due to operational changes **(W)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
	procedures to audit and monitor activities performed by PeopleSoft administrators.	monitoring activities performed by those that have System Administrator rights to deter and detect any inappropriate activities in PeopleSoft. This will be completed by 1st quarter 2015.			department management, which delayed implementation.
5.1	Internal Audit recommends management coordinate with IT and periodically test and update its business continuity plan. The frequency of such tests should be dictated by system criticality and should occur at least every 12-18 months.	A Business Continuity Plan will involve planning and discussion outside of HRMS, Finance and IT. Management has begun conversations with the Server team and provided the following time line for a Disaster Recovery plan as it relates to the system.	05/2015	I	

DATE	MILESTONE
09-Feb	Project Start
27-Feb	Server Build
13-Mar	Software Installation
06-Apr	Data Load
20-Apr	Data Replication
04-May	Testing Complete
24-May	Failover Test