Mecklenburg County
Department of Internal Audit

PeopleSoft Application Security Follow-Up Audit
Report 1917

May 14, 2020

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA, CIA, CFE, CFF, CRMA, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Deborah Caldwell, CISA, CIA, Information Technology Auditor
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: Joanne Prakapas, Director
Department of Internal Audit

Date: May 14, 2020

Subject: PeopleSoft Application Security Audit Follow-Up Audit Report 1917

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Fiscal Year	Audit Report	Implemented	Open	Not Implemented[1]	Withdrawn	Total Carryforward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

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

The attached **Follow-Up Results** matrix provides details for the most recent follow-up audit. Internal Audit will review any carryforward issues later to verify recommendations are fully implemented and working as intended.

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 of the policy and associated	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 regarding application security risk assessments and business continuity planning were under development but not complete. Human Resource management has implemented a new management structure and organized resources with a specific focus on HRMS related activities and implementation of risk mitigation strategies.

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**
	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	P (2)	Management indicated the recommendations have been implemented and are pending Internal Audit's review.
4.1	Internal Audit recommends management define and implement procedures to audit and monitor	HRMS, Finance and IT will define how to move forward with auditing and monitoring activities performed by	03/2015	P	Management indicated the recommendation has been implemented and is pending Internal Audit's review.

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)**

<table>
<tr><th></th><th></th><th></th><th></th><th colspan="2">Implementation Status</th></tr>
<tr><th>Risk Observation</th><th>Recommendation</th><th>Management’s Risk Mitigation Strategy</th><th>Original Implementation Date</th><th>Current Status</th><th>Comments</th></tr>
<tr><td></td><td>activities performed by PeopleSoft administrators.</td><td>those that have System Administrator rights to deter and detect any inappropriate activities in PeopleSoft. This will be completed by 1st quarter 2015.</td><td></td><td></td><td></td></tr>
<tr><td>5.1</td><td>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.</td><td>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.
<table>
<tr><th>DATE</th><th>MILESTONE</th></tr>
<tr><td>09-Feb</td><td>Project Start</td></tr>
<tr><td>27-Feb</td><td>Server Build</td></tr>
<tr><td>13-Mar</td><td>Software Installation</td></tr>
<tr><td>06-Apr</td><td>Data Load</td></tr>
<tr><td>20-Apr</td><td>Data Replication</td></tr>
<tr><td>04-May</td><td>Testing Complete</td></tr>
<tr><td>24-May</td><td>Failover Test</td></tr>
</table></td><td>05/2015</td><td>P</td><td>Internal Audit determined the recommendation is partially implemented due to Information Technology Service’s timeline to plan and test PeopleSoft recovery.</td></tr>
</table>