Mecklenburg County
Department of Internal Audit

PeopleSoft Application Security Audit Follow-Up Audit
Report 1585

April 19, 2016

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CFE, 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	Rick Kring, CISA, Auditor-In-Charge Deborah Caldwell, CIA, CISA, Information Technology Auditor
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at http://charmeck.org/mecklenburg/county/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Dena Diorio, County Manager

From: Joanne Prakapas, Director, Department of Internal Audit

Date: April 19, 2016

Subject: PeopleSoft Application Security Audit Follow-Up Audit Report 1585

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 objective of the follow-up audit 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 and 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 summarizes the results of the follow-up audits performed to date.

Recommendation Summary					
Fiscal Year	**Audit Report**	**Implemented**	**Open**	**Not Implemented**	**Withdrawn**
2015	1585	5	6		

Details regarding the most recent follow-up audit are noted in the attached **Follow-Up Results** matrix. Recommendations considered implemented will be excluded from further review. For those that remain open, Internal Audit will conduct a follow-up audit at a later date to verify they are fully implemented and working as intended.

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

c: Deputy County Manager/Chief of Staff
Assistant County Managers
Deputy 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	Management indicated the recommendation is partially implemented due to competing priorities and changes in staff and department management. Since the completion of audit fieldwork, management indicates the risk mitigation strategy is implemented and 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)**

				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				
1.2	Internal Audit recommends management develop a formal, documented process to periodically review, modify, and approve as necessary PeopleSoft policies and procedures. The written policies and procedures should have a framework that establishes, at a minimum: • Frequency of reviews • Staff roles and responsibilities • Staff training requirements • Communication requirements for internal and external stakeholders		03/2015	P	Management indicated the recommendation is partially implemented due to competing priorities and changes in staff and department management. Since the completion of audit fieldwork, management indicates the risk mitigation strategy is implemented and pending Internal Audit's review.
2.1	Internal Audit recommends management work with the Payroll Division to ensure PeopleSoft access request forms are appropriately completed, reviewed, and approved. In addition, access request that are not properly completed or approved should be returned to the originator for correction prior to granting access.	Create and implement the following by 1st Quarter 2015: • Document and enforce our Standard Security Process. This will ensure that the necessary signatures, approvals are in place prior to granting access to PeopleSoft. • Communicate form and process to managers via meckweb and myHR portal. Currently, HRMS runs a biweekly report that	03/2015	I (2)	

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**
		considers changes in a user's job responsibilities. We use this report to remove access that is no longer needed. HRMS will document this process. When a user changes job responsibilities and may need additional access we expect a form to be completed and submitted to HRMS by the employee's manager. This expectation will be included in our standard security process.			
2.2	Internal Audit recommends management work with the Payroll Division to establish an annual recertification process for PeopleSoft user access privileges.	Establish an annual recertification process for those employees (users) that have access outside of the common "employee" role. This process will be defined and documented by 1st quarter 2015.	03/2015	I	
2.3	Internal Audit recommends management limit the number of users assigned the System Administrator role, applying the least-privilege use principle.	We will review users that have the System Administrator role. We agree that this privilege access should be limited in production and we will determine access rights based on roles by the end of 2nd quarter 2015. We do find that System Administrator rights are a necessity for upgrading the system, testing, troubleshooting and exploring additional functionality in our test environments.	06/2015	I	

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**
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 recommendation is partially implemented due to competing priorities and changes in staff and department management. Since the completion of audit fieldwork, management indicates the risk mitigation strategy is implemented and pending Internal Audit's review.
4.1	Internal Audit recommends management define and implement procedures to audit and monitor activities performed by PeopleSoft administrators.	HRMS, Finance and IT will define how to move forward with auditing and 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.	03/2015	P	Management indicated the recommendation is partially implemented due to competing priorities and changes in staff and department management. Since the completion of audit fieldwork, management indicates the risk mitigation strategy is implemented and 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)**

				Implementation Status	
Risk Observation	**Recommendation**	**Management's Risk Mitigation Strategy**	**Original Implementation Date**	**Current Status**	**Comments**
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. **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	05/2015	P	Management indicated the recommendation is partially implemented due to Information Technology's timeline to plan and test PeopleSoft recovery in FY2017.
6.1	Internal Audit recommends management change PeopleSoft password settings to align with leading best practice values.	HRMS, Finance and IT will discuss best practices recommended for password settings and determine the configuration set-up to implement by 1st Quarter 2015.	03/2015	I	