Mecklenburg County
Department of Internal Audit

PeopleSoft Application Security Audit
Report 1452

February 9, 2015

Internal Audit's Mission	Through open communication, professionalism, expertise and trust, Internal Audit assists executive management and the Audit Review Committee in accomplishing the Board's objectives by bringing a systematic and disciplined approach to evaluate the effectiveness of the County's risk management, control and governance processes in the delivery of services.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CFE, CRMA, Audit Director (980) 314-2889 or joanne.whitmore@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Richard Kring, 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: Chris Peek, Deputy County Manager/Chief of Staff and Director, Human Resources Department

From: Joanne Prakapas, Director, Department of Internal Audit

Date: February 9, 2015

Subject: PeopleSoft Application Security Report 1452

The Department of Internal Audit has completed its audit of PeopleSoft, Mecklenburg County's human resource management system. The audit objective was to determine whether internal controls effectively managed key risks inherent to PeopleSoft application security. Specific areas of focus included access management, configuration management, change management, and business continuity. Internal Audit interviewed key personnel, observed operations, reviewed and evaluated policies and procedures, performed data analytics, and assessed the operating effectiveness of the provisioning and de-provisioning processes.

This audit was conducted in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

OVERALL EVALUATION

Overall, the management of risks inherent to PeopleSoft application security requires improvement in the design and operation of some control activities.

RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during the course of the audit, grouped by the associated risk factor and defined in Appendix A. The criticality or significance of each risk factor, as well as Internal Audit's assessment of the design and operation of key controls to effectively mitigate the risks, are indicated by the color codes described in Appendix B.

RISK OBSERVATION SUMMARY			
Risk Factors and Observations	**Criticality**	**Design**	**Operation**
1. Policies and Procedures Risk	🔴	🔴	🔴
1.1 Formal Documentation 1.2 Review and Approval			
2. System Access Risk	🔴	🟡	🟡
2.1 Management Authorization 2.2 User Recertification 2.3 Least-Privilege			
3. Segregation of Duties Risk	🔴	🟡	🟡
3.1 Access Privileges			
4. System Auditing / Monitoring Risk	🟡	🔴	🔴
4.1 PeopleSoft Administrators			
5. System Contingency Risk	🟡	🟡	🔴
5.1 Business Continuity Planning			
6. System Configuration Risk	🔴	🟡	🔴
6.1 Password Settings			

The risk observations and management's risk mitigation strategies are discussed in detail in the attached document. Internal Audit will conduct a follow-up review at a later date to verify management's action plans have been implemented and are working as expected.

We appreciate the cooperation you and your staff provided during this audit. Please feel free to contact me at 980-314-2889 if you have any questions or concerns.

c: County Manager
Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee

BACKGROUND

PeopleSoft is an Enterprise Resource Planning system that allows for the integration of business functions and a single access control model. The County uses the PeopleSoft Enterprise system for a variety of key business functions, such as human resource administration and payroll processing. The Human Resources Department (the Department) is a key business owner and primary user of PeopleSoft, and their system administrators provide support for key system activities, such as:

- User definition, maintenance, and application level security
- Business process definitions and maintenance of business rules
- Production processing support
- Coordination of technical configuration, application software maintenance, and database support

The County's Information Technology Department (IT) provides technical support for PeopleSoft, which includes enterprise-wide network security and configuration management, database management, and disaster recovery.

Application Level General Controls

Application level general controls are policies and procedures specific to an application and include activities related to security management, system access, configuration management, segregation of duties, and business continuity. These controls help management assure the confidentiality, integrity, and availability of information assets. They also provide reasonable assurance that application resources and data are protected against unauthorized modification, disclosure, loss, and/or impairment.

User Access

Employees are granted access rights to the PeopleSoft system upon being hired. Job requirements determine additional access rights and such rights are modified when job responsibilities change. Access is disabled or removed when individuals terminate their employment with the County.

Security Administration

User access to data within PeopleSoft is primarily controlled by assigning roles to the user. In turn, roles have assigned permission lists that define what pages can be accessed and how the data on the page can be accessed. Data access can vary from allowing a user read-only access at the low end to the ability to correct data at the high-end. Permission lists can access from tens to hundreds of data items. Users can have multiple roles and roles can have multiple permission lists. It is also possible to assign a permission list directly to a user, rather than to the user's role.

Configuration Management

The County's PeopleSoft installation includes three environments:

- Development
- Quality Assurance / Test (QA)
- Production

To protect the integrity of the production environment, programmers use a development environment to make changes and updates to PeopleSoft. Business analysts from the Human Resources and Financial Services Department perform functionality, processing, and testing in the quality assurance environment, and decide when changes and updates are ready to migrate to the production environment. Migrations to the production environment are performed by the PeopleSoft administrators or a designee.

COUNTY MANAGER'S OVERALL RESPONSE

The County Manager concurs with all risk mitigation strategies and timeframes for implementation.

RISK OBSERVATIONS AND MITIGATION STRATEGIES

Risk Factor	Criticality	Design	Operation
1. Policies and Procedures Risk	🔴	🔴	🔴

Risk Observations

1.1 Formal Documentation—While many of the appropriate activities are carried out to manage PeopleSoft, the Department is highly reliant on individuals' knowledge of proper procedures. In many instances, supporting policies, procedures, and/or standards do not exist to provide formal structure around key activities. Yet, policies, procedures, and standards are important control activities to help management ensure its directives are carried out while mitigating risks that may prevent the department from achieving its objectives.

PeopleSoft activities impacted include but are not limited to:

- Application security management
- System and security configuration standards
- System monitoring and auditing
- Service and data administrator roles and responsibilities
- Business continuity planning

1.2 Review and Approval—Management does not evidence their periodic review and approval of written PeopleSoft access procedures to ensure they are up-to-date and reflect current and best practices, as well as changes in technologies, operations, laws, regulations, and standards. Periodic evaluations and updates provide management a level of assurance that control activities are functioning as intended.

Recommendations

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 (UserID) and password management; system delivered UserIDs; 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 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

Management's Risk Mitigation Strategy

1.1/1.2 HRMS[1], 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. Projected implementation date is March 31, 2015.

Risk Factor	Criticality	Design	Operation
2. System Access Risk			

Risk Observations

2.1 Management Authorization—Management approvals for PeopleSoft access were not consistently documented prior to granting access. Review of 65 employee access requests disclosed 29 or 45% were not properly authorized with a signature from an appropriate departmental official. In addition, 12 PeopleSoft access requests specific to payroll-related functions did not evidence the required approval from the Financial Services Department's Payroll Division (the Payroll Division). Without appropriately documenting user access authorization, management has limited ability to ensure employee access privileges do not exceed that necessary to carry out their job duties.

2.2 User Recertification—PeopleSoft user access privileges were not reviewed on a periodic basis to ensure the level of privileges remained appropriate. The lack of a periodic review of user access privileges increases the risk that excessive or inappropriate access privileges will not be timely detected or removed.

2.3 Least-Privilege—The PeopleSoft System Administrator role is a privileged user role, which allows the user access to sensitive application resources, such as password files, data modification rights, and security administration. The Department does not, however, limit the PeopleSoft System Administrator role to only those employees who must have such privileges to perform their duties. Rather, 11 users have this elevated access. Best practice suggests using a delegation model applying the least-privilege principle to enforce specific roles and limit the number of individuals assigned such privileges.

[1] HRMS : The Human Resources Management System division; IT: Information Technology Department; Finance: County Financial Services

Recommendations

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.

2.2 Internal Audit recommends management work with the Payroll Division to establish an annual recertification process for PeopleSoft user access privileges.

2.3 Internal Audit recommends management limit the number of users assigned the System Administrator role, applying the least-privilege use principle.

Management's Risk Mitigation Strategy

2.1 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 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 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.

2.3 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.

Risk Factor	Criticality	Design	Operation
3. Segregation of Duties Risk	🔴	🟡	🟡

Risk Observation

3.1 Access Privileges—Some access privileges in the PeopleSoft quality assurance and production environments did not enforce appropriate segregation of duties to diminish the likelihood that errors and wrongful acts will go undetected. Specifically, two individuals have "Application Designer" and "Data Mover" roles in the quality assurance environment. The same individuals also have the "Designer" role in the production environment. As a result, they can both change production data and perform updates to production data.

Recommendation

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.

Management's Risk Mitigation Strategy

3.1 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.

Risk Factor	Criticality	Design	Operation
4. System Auditing / Monitoring Risk			

Risk Observation

4.1 System Administrators—Specific monitoring controls were not in place to review transactions or activities performed by PeopleSoft system administrators. As a result, inappropriate use may not be deterred or timely detected.

Recommendation

4.1 Internal Audit recommends management define and implement procedures to audit and monitor activities performed by PeopleSoft administrators.

Management's Risk Mitigation Strategy

4.1 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.

Risk Factor	Criticality	Design	Operation
5. System Contingency Risk	🟡	🟡	🔴

Risk Observation

5.1 Business Continuity Planning—The Department has not updated and tested its business continuity plan or verified with IT that PeopleSoft can be timely recovered and resume functionality in the event of an emergency. Periodic testing of business continuity plans is an essential part of disaster recovery planning to ensure the plan will work when needed.

Recommendation

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.

Management's Risk Mitigation Strategy

5.1 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

Risk Factor	Criticality	Design	Operation
6. System Configuration Risk			

Risk Observation

6.1 Password Settings—PeopleSoft password settings were not fully aligned with leading practices. Failure to establish effective password settings increases the risk passwords may be compromised and allow unauthorized access. For example:

- The number of previous passwords used to determine if a changed password is permitted was set to zero, where best practice suggests eight
- The number of tries a user is allowed to complete a successful log on (valid UserID and matching password) was set to 50 attempts where best practice suggests five attempts
- The number of characters required to create an acceptable password was set to five where best practice suggests eight
- Minimal level of password complexity is disabled but should be enabled

Recommendation

6.1 Internal Audit recommends management change PeopleSoft password settings to align with leading best practice values.

Management's Risk Mitigation Strategy

6.1 HRMS, Finance and IT will discuss best practices recommended for password settings and determine the configuration set-up to implement by 1st Quarter 2015.

APPENDIX A—Risk Factor Definitions

Risk Factor	Definition
Policies and Procedures Risk	Policies and procedures that are non-existent, ineffective, unclear, or outdated may result in poorly executed processes and increased operating costs.
System Access Risk	Failure to appropriately restrict access to data or programs may result in unauthorized changes to data or programs, inappropriate access to restricted or confidential information, or inefficiencies where access is too restrictive.
Segregation of Duties Risk	Inadequate segregation of duties may allow individuals to carry out inappropriate activities without timely detection.
System Auditing / Monitoring Risk	Failure to identify and log incidents and/or conduct effective analysis and take appropriate actions may allow unauthorized access to information system resources to go undetected and/or be untimely detected.
System Contingency Risk	Failure to proactively manage system contingencies may result in service interruptions that significantly impact the organizations' ability to process, retrieve, and protect electronically maintained information.
System Configuration Risk	Lack of effective configuration management processes may result in systems that do not perform as intended to support operation of critical processes.

APPENDIX B—Color Code Definitions

The criticality of a risk factor represents the level of potential exposure to the organization and/or to the achievement of process-level objectives before consideration of any controls in place (inherent risk).

Criticality	Significance and Priority of Action
🔴	The inherent risk poses or could pose a ***significant*** level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take immediate action to address risk observations related to this risk factor.
🟡	The inherent risk poses or could pose a ***moderate*** level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take prompt action to address risk observations related to this risk factor.
🟢	The inherent risk poses or could pose a ***minimal*** level of exposure to the organization and/or to the achievement of process level objectives. Risk observations related to this risk factor, however, may provide opportunities to further reduce the risk to a more desirable level.

The assessment of the design and operation of key controls indicates Internal Audit's judgment of the adequacy of the process and system design to mitigate risks to an acceptable level.

Assessment	Design of Key Controls	Operation of Key Controls
🔴	The process and system design does not appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities is not consistently effective to manage the risk to an acceptable level.
🟡	The process and system design appear to be adequate to manage the risk to an acceptable level. Failure to consistently perform key risk management activities may, however, result in some exposure even if other tasks are completed as designed.	The operation of the process' risk management capabilities is only partially sufficient to manage the risk to an acceptable level.
🟢	The process and system design appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities appears to be sufficient to manage the risk to an acceptable level.