Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Audit Team on the Engagement:
Kim Anderson, PwC
Chris Bevan, PwC
Jonny Brennan, Undergraduate Student Intern
Jacob L. Claeys, CGAP, CRMA, CICA
Shayna Gilbert, Undergraduate Student Intern
Charlie Lallas, PwC
Magdy Mossaad, MBA, CIA, CMA, CFE, CPA

Application Security Review

Published by Order of Audit Committee on March 27, 2013

Report # 2013–02

Minneapolis
City of Lakes

Date: March 27, 2013

To: Kevin Carpenter, Finance & Property Services Department (FPS)
Otto Doll, Information Technology Department (IT)
Tim Giles, Human Resources Department (HR)

Re: Application Security Review

The Internal Audit Department (IA) contracted with PricewaterhouseCoopers (PwC), one of the Big 4 audit firms, to collaboratively conduct an Application Security review of the PeopleSoft system for the City of Minneapolis (City). This review was included in the 2012 Internal Audit Plan.

Background
The City utilizes PeopleSoft applications to support key financial and human resource transactions. The PeopleSoft Compass system houses the general financial transactions while the PeopleSoft Human Resources Information System (HRIS) manages payroll, benefits and human resources.

Objectives
The objectives of this review include the following: (1) to determine the current access of City employees for specified PeopleSoft software applications and assess whether appropriate controls are in place to prevent and detect inappropriate access to these PeopleSoft applications; (2) to review internal policies and procedures in order to assess the adequacy of controls over access management; and finally,(3) to assess whether access is appropriate, users are current and there is an appropriate level of segregation of duties.

Scope
This review was limited to the following applications:
1. General Ledger (PeopleSoft Version 9.0, PeopleTools Version 8.49.25)
2. Accounts Payable (PeopleSoft Version 9.0, PeopleTools Version 8.49.25)
3. Accounts Receivable (PeopleSoft Version 9.0, PeopleTools Version 8.49.25)
4. Payroll and HR Job data access that is pay related (PeopleSoft Version 8.9, PeopleTools Version 8.49.28)
5. Time and Labor (T&L) (PeopleSoft Version 8.9, PeopleTools Version 8.49.28)

Approach
1. Performed a risk assessment to determine key financial transactions and their related access within the General Ledger, Accounts Payable, Accounts Receivable, Payroll, T&L, and HR processes.

2. Collaborated to gain an understanding of the aforementioned PeopleSoft processes by performing a high-level process walk-through, including reviewing existing documented PeopleSoft access policies and procedures.

3. Assessed the operating effectiveness of the provisioning and de-provisioning processes for the in-scope applications. Collaborated with IA and applicable department management to confirm exceptions to the processes.

4. Utilized PwC's proprietary tool, PeopleSoft GATE, to perform an automated assessment to determine individuals with access to transactions. PwC ran the tool on all access areas and provided the results to IA and applicable department management for future process assessments.

5. If results did not meet expectations of duties that should be segregated or restricted, with IA, PwC met with applicable City department management to discuss results and next action steps to address the expectation gap.

Summary of Findings *and Management Responses:*

1. Application Security Policy

The security of the applications within each of the PeopleSoft environments (Compass and HRIS) is administered by separate business and technology support teams which work with the City's IT Department to operate and maintain the systems. Application security standards within the PeopleSoft environments are not consistent and could be improved.

Management Response

FPS and Human Resources Technology Solutions (HRTS) will work with IT to develop individual System Security Plans that address these system security protocols and procedures for Compass HRTS.

2. Segregation of Duties (SoD) Framework and Monitoring

It was noted that segregation of duties is important to each of the departments within the scope of this review, and is a primary factor underlying the implementation of and documented within multiple policies, procedures, and internal control processes and monitoring. However, a formal documented segregation of duties framework for systems security access is not readily available.

Management Response

FPS and HRTS will document and incorporate into a related Internal Control document the basic standards/principles underlying the SoD framework for determining access to the systems including the identification of user preferences and other mitigating controls that assist in ensuring appropriate access and use of the systems is properly assigned and/or regularly reviewed and monitored. In addition FPS and HRTS will develop and document in the Internal Control document processes to review and monitor access roles on a periodic basis to ensure individuals have appropriate access.

3. Additions and Separated Employee Processes

It was noted that approvals were not consistently obtained prior to access being granted to the system. Also, City terminated employees were not consistently removed timely from the PeopleSoft systems.

Management Response

HRTS or Compass Support can add a step in the separation process to run a weekly separation list from the system. With that list, FPS can update Compass user access accordingly. In addition, HRTS performs a bi-monthly audit of employees who transfer or move positions. HRTS notifies the department contact and changes the employees' security accordingly. This may also be helpful to FPS Compass Support in monitoring system access to Compass.

4. Compass and HRIS Super Users

Several IT and non-IT users have super user access within the Compass and HRIS system. Super users have access to perform all activities within the system, which allows them to bypass SoDs and application controls. Specific monitoring controls are not in place to review transactions or activities performed by these users to ensure that only appropriate transactions occur.

Management Response

HRTS and Compass Support will review users assigned to this access and determine if the users require this access for their job responsibilities. Both HRTS and FPS Compass Support will establish security tables/audit logs that can be monitored periodically on a regular basis to ensure system access is appropriate.

Conclusion
Based on our review, we believe there are opportunities for improvements to address risk areas identified in this report. FPS, HR and IT worked collaboratively with IA to develop action plans to address these risks.

IA and PwC would like to extend our appreciation to FPS, HR and IT personnel who assisted and cooperated with us during this review.

Cc: Paul Aasen, City Coordinator's Office
Sandra Christensen, FPS
Lalonnie Erickson-Baker, FPS
Connie Griffith, FPS
Rich Martonik, HR
Randy Mikkelson, IT
Ray Morales, FPS
Deb Parker, IT

Application Security Review
Audit Findings and Management Responses

1. Application Security Policy

The City has not published a formal written application security policy. The security of the applications within each of the PeopleSoft environments (Compass and HRIS) is administered by separate business and technology support teams which work with the City's IT Department to operate and maintain the systems. In the review, we determined that application security standards within the PeopleSoft environments are not consistent and could be improved. An application security policy that applies to all systems within the City would help to ensure that strong application security standards are consistently applied to all system environments, and appropriate protocols and procedures are established to help ensure that only appropriate external or internal individuals are able to access the systems. In our review of the current application security protocols and procedures, we noted that improvements could be made in the following areas: (1) password parameters; (2) retained default User Identifications (Ids); (3) assignment of generic Ids; (4) periodic access reviews; and, (5) assessment of public-facing applications.[1]

Recommendation

We recommend that FPS, HR and IT management collectively develop an application security policy that can be applied to multiple applications and departments. This policy should address the acceptable usage of the applications and the minimum security requirements for the City. Additionally, the policy should reference specific protocols and procedures that address the following:

1. Password parameters including consideration of the use of strong passwords that require such things as the use of a special digit and/or character, lockout after a certain number of failed attempts, and a minimum length of at least 6 characters.
2. Maintenance, assignment, and monitoring of Default Ids created during system implementation or with the addition of new automatic system accesses and used on an ongoing basis to manage system performance and automated system processes.
3. Maintenance, assignment and monitoring of Generic Ids used in lieu of person specific user identification for system maintenance and other automated system processes.
4. Development of methodologies to periodically review/monitor system access to ensure that access is and continues to be aligned with an employee's job responsibilities.
5. Review and evaluate PeopleSoft public-facing applications (such as web access to HRIS or the Compass system) to ensure that private City data is protected.

Management Response

FPS and HR will work with IT to develop individual System Security Plans that address these system security protocols and procedures for Compass and HRTS. This collaborative approach will enable FPS and HR to address inconsistencies between the two systems while enabling each to establish protocols, procedures and minimum standards specific to each of the systems and processes in a planned, purposeful way. The System Security Plans can address the roles, responsibilities, security requirements, controls and operating procedures more directly for the system in question.

The IT Department is responsible for drafting IT application security policy at the enterprise governance level. HR and FPS will be among the stakeholders consulted in the development of such policy.

Responsible Party
IT – Deb Parker
HRTS – Rich Martonik

[1] For the purposes of this report, a public-facing application refers to the PeopleSoft applications that can be accessed outside of the City network.

FPS – Lalonnie Erickson-Baker and Compass Support

Expected Completion Date
End of 2nd Quarter 2014 for the System Security Plans.

Projected Cost of Implementation
IT: 100 to 160 hours; $6,250 to $10,000
HRTS: 80 to 120 hours; $2,700 to $5,400
FPS: 80 to 120 hours; $5,200 to $7,800

2. Segregation of Duties (SoD) Framework and Monitoring

Auditors performed walk-throughs and interviews surrounding the segregation of duties framework for the system security access within the City's FPS, HR and IT departments. It is noted that segregation of duties is important to each of the departments within the scope of this review, and is a primary factor underlying the implementation of and documented within multiple policies, procedures, and internal control processes and monitoring. However, a formal documented segregation of duties framework for systems security access is not readily available. A formal segregation of duties framework should contain the duties that are expected to be separated within the system, including the detailed activities users should not have conflicting access to. The SoD framework should identify compensating controls for instances in which segregation cannot be achieved and the conflicting access is assigned. By not documenting the criteria underlying the segregation of duties framework, there is an increased risk that conflicting access could be assigned and ultimately, fraudulent transactions could occur. For example, while this level of access was not noted during this audit in the City's HRIS or Compass system, an individual could hire a fictitious employee, assign an insignificant compensation rate and pay themselves. During our assessment, it was noted that access appeared to be restricted in critical segregation of duties instances; however, enhancements could be made over end user security to ensure adequate segregation of duties exists. Additionally, in the few instances in which conflicting access appeared excessive, it was generally assigned to the individuals with super user access as noted in Audit Finding #4.

Recommendation

We recommend that FPS, HR and IT management create a formal documented SoD framework for system security access to aid the Compass and HRTS support team in preventing conflicting duties to be assigned upon initial systems access request. This could help to prevent unwarranted excessive access from being assigned to end users, and act as a catalyst for periodic access reviews. During the users reviews, the applicable departments should also assess each critical activity to determine if access appears excessive based on their expectations. If this access is not appropriate, management should remove this access. Additionally, management should assess access to all pages, even if the page[2] is not the typical path used to gain access, to ensure that users cannot haphazardly obtain access to functions that are not aligned with their job responsibilities. Additionally, management can enhance the SoD framework by leveraging existing mitigating and monitoring controls to document their response to the specific SoD risks. Once the framework has been established, periodic monitoring should be put into place to ensure that conflicting access is not assigned and / or appropriate mitigating controls exist.

Management Response

The City has a strong SoD framework that is formally captured in policy, organization structure, documentation of operating procedures and processes, internal control and risk assessment documentation, and workflow processes built into the systems. Requests for access are required to have both a written department and finance manager or HRG approval. Access "roles" are assigned based on business need and job assignments and responsibilities. User preferences are used to further limit the access based on factors including SoDs. Roles are designed to be relatively broad in definition with user preferences providing the limitations needed to meet system security standards

[2] A PeopleSoft page is the screen in which a user can perform an activity and/or transaction within the system.

and address such things as SoDs. In addition, there are other internal controls in place outside of the system security access standards that help to mitigate the risk inherent in what may appear to be "excessive" access.

Both teams will document and incorporate into a related Internal Control document the basic standards/principles underlying the SoD framework for determining access to the systems including the identification of user preferences and other mitigating controls that assist in ensuring appropriate access and use of the systems is properly assigned and/or regularly reviewed and monitored. In addition both teams will develop and document in the Internal Control document processes to review and monitor access roles on a periodic basis to ensure individuals have appropriate access.

Responsible Party
HRTS – Rich Martonik
FPS – Lalonnie Erickson-Baker and Compass Support

Expected Completion Date
HRTS: End of 4th Quarter 2013
FPS: End of 2nd Quarter 2014

Projected Cost of Implementation
HRTS: 80 to 120 hours; $2,700 to $5,400
FPS: One time: 120 to 160 hours (staff); 120 hours (consultant); $19,800 to $22,400
Ongoing: 8 hours/quarter; $2,080 annually

3. Additions and Separated Employee Processes

To gain access to Compass or HRIS, a security form must be completed with the appropriate authorizations obtained prior to access being granted. Auditors performed detailed testing over this process and noted that approvals were not consistently obtained prior to access being granted to the system. Without appropriate approvals, access could be haphazardly assigned that may not align with the user's job responsibilities.

City terminated employees were not consistently removed timely from the PeopleSoft systems. The process to remove access is automated and is based on the date the separation row is added in HRIS, not the effective date of the separation. Therefore, this process relies heavily on HR to notify the appropriate stakeholders of the individual's separation. If access to the system is retained beyond an employee's separation date, private data could be compromised and inappropriate financial transactions may occur. Auditors performed testing to determine if any separated employees from 2012 still retained access to the PeopleSoft system. Auditors noted that, during the procedures performed, 11 Compass users retained system access after separation and 58 HRIS users retained system access outside of their 30 day termination allowance window. It was noted that processes are in place to monitor separated HRIS users; however, this should be formalized and run on a regularly scheduled basis.

Recommendation

We recommend the City enhance its processes to ensure that all applicable departments, Compass and HRTS support are notified when an individual is separated. As Compass and HRIS contain sensitive data, these systems should be added to existing processes to ensure adequate removal. Additionally, the Compass system could receive periodic updates from HR regarding separations for the month to identify any employees that were not provided for immediate removal.

Management Response

HRTS or Compass Support can add a step in the separation process to run a weekly separation list from the system. With that list, FPS can update Compass user access accordingly. In addition, HRTS performs a bi-monthly audit of employees who transfer or move positions. HRTS notifies the

department contact and changes the employees' security accordingly. This may also be helpful to FPS Compass Support in monitoring system access to Compass.

In addition, IT is implementing an Identity Management System that will automate management of network and other systems access accounts. If funding can be procured, they are targeting 2014 to implement the phase of the project that will integrate HRIS into the system so that new, departing and employee job change events will kick off automated workflows for managers to make and implement access and authorization changes based on HRIS employee status.

Responsible Party
IT – Deb Parker
HRTS – Rich Martonik
FPS – Lalonnie Erickson-Baker and Compass Support

Expected Completion Date
End of 3rd Quarter 2013

Projected Cost of Implementation
IT: Implementing an Identity Management System is projected to cost $150,000 to $200,000
HRTS: 40 hours; $1,800
FPS: One time: 40-80 hours; $2,600 - $5,200
Ongoing: 4 hours/month; $3,120 annually

4. Compass and HRIS Super Users

Several IT and non-IT users have super user access within the Compass and HRIS system. Super users have access to perform all activities within the system, which allows them to bypass SoDs and application controls. Specific monitoring controls are not in place to review transactions or activities performed by these users to ensure that only appropriate transactions occur. For example, one Park Board user was provided excessive access to all functions within the Compass system, including IT functions. This user could have performed unapproved transactions without the proper monitoring.

Recommendation

FPS, HRTS and IT management should consider the following best practices:

1. Restrict super user access to only those who require it. Such access is typically needed only by system support staff.
2. Review current access configurations and determine if individual access is aligned with job responsibilities. Reconfigure access to remove super user privileges where appropriate. IA has provided management with detailed recommendations for suggested configuration changes.
3. Define a procedure to create temporary super user accounts for staff who do not need such access as part of routine job duties. These accounts could only be made active within the system after an approval from management is obtained. Once access is no longer required, this access should be removed and the password changed. Management would discuss activities that were performed and note it within the request for tracking purposes.
4. Monitor activities performed by super users to detect unauthorized use of super user privileges. Consider automated monitoring that would alert management to high risk activities such as: vendor creation, journal entries, employee payments, vendor payments, employee creation, etc.

Management Response

HRTS and Compass Support will review users assigned to this access and determine if the users require this access for their job responsibilities. We will also review the access assigned within these roles to determine if any "risky" access can be removed. Both HRTS and FPS Compass Support will

work with IT to develop security tables/audit logs and related reports that track super user access activities that can be monitored periodically on a regular basis to ensure system access is appropriate.

Responsible Party
IT – Deb Parker
HRTS – Rich Martonik
FPS – Lalonnie Erickson-Baker and Compass Support

Expected Completion Date
End of 4th Quarter 2013

Projected Cost of Implementation
IT: $20,000 to $200,000 depending on the complexity of the customization required to track the super user's activities and whether or not an additional or new software solution is required.
HRTS: 40 hours; $1,800
FPS: On-going monitoring: 2 hours/month; $1,560 annually

Projected Cost of Implementation (contents provided by FPS, HRTS & IT)				
Audit Finding		Total Estimated Cost		
		FPS	HRTS	IT
1	Application Security Policy	$5,200 to $7,800	$2,700 to $5,400	$6,250 to $10,000
2	Segregation of Duties (SoD) Framework and Monitoring	$19,800 to $22,400 $2,080 (annually)	$2,700 to $5,400	-
3	Additions and Separated Employee Process	$2,600 to $5,200 $3,120 (annually)	$1,800	$150,000 to $200,000
4	Compass and HRIS Super Users	$1,560 (annually)	$1,800	$20,000 to $200,000
	Total (one time)	$27,600 to $35,400	$9,000 to $14,400	$176,250 to $410,000
	Total (annually)	$6,760	-	$230,000*

*** IT will need a Security Engineer and Security Application Analyst for implementing and maintaining proposed security systems**

Abbreviations Used Throughout the Report	
City	The City of Minneapolis
Compass	City's Accounting system
FPS	Finance and Property Services Department
HR	Human Resources Department
HRIS	Human Resources Information System
HRTS	Human Resources Technology Solutions
IA	Internal Audit Department
Ids	User Identifications
IT	Information Technology Department
PeopleSoft GATE	A PwC proprietary tool used to perform an automated assessment to determine individuals with access to transactions.
PwC	PricewaterhouseCoopers
SoD	Segregation of Duties
T&L	Time and Labor (T&L) is a module in the PeopleSoft HRIS that provides City employees the ability to report their timesheet online.