CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

HIGHLIGHTS

Highlights of City Auditor Report #1706, a report to the City Commission and City management

April 7, 2017

AUDIT OF THE CLOUD MIGRATION & UPGRADE TO PEOPLESOFT SYSTEMS

The City successfully migrated (transitioned) the PeopleSoft Financials and Human Resources systems to a cloud environment. However, efforts to subsequently upgrade the two City systems to current versions were temporarily suspended.

WHY THIS AUDIT WAS CONDUCTED

This audit was conducted to evaluate and report on management's efforts to transition the City's PeopleSoft Financials and Human Resources (HR) systems to a cloud environment and to subsequently upgrade those two major systems. Because this major information technology project (Project) is anticipated to take more than two years to complete, this audit is being conducted in two phases. This report covers the first phase, which is represented by the period from the start of the Project through completion of the transition, or migration, of the two systems from an internally managed environment to a cloud environment. The second phase will address the City's remaining efforts to upgrade the two systems subsequent to the cloud migration.

WHAT WE FOUND

1. The City's PeopleSoft Financials and HR systems were successfully migrated to and are currently operating in a cloud environment.
2. The City followed and met most of the best practices identified for successful migrations to a cloud environment, and did not suffer any identifiable adverse impacts for the practices not initially followed or met.
3. Efforts to subsequently upgrade the two City systems to current versions were suspended due to challenges resulting from a lack of clarity and specificity in certain contractual terms and conditions regarding roles and responsibilities of City and contractor staff.
4. Payments totaling $1.2 million made by the City to contracted Project vendors were generally correct; however, enhanced Project planning and scheduling, as well as stronger negotiation and contractual restrictions, would likely have reduced those costs. Also, an inadequate understanding of certain contractual provisions resulted in an undetected overbilling and overpayment for hosting services.
5. It likely would have been more beneficial to the City if competitive proposals had been solicited and evaluated in connection with the selection of Project contractors.
6. The contract for upgrade services should have been structured differently to reduce the City's exposure to certain financial risks.
7. Cloud hosting costs associated with the transitioned systems are expected to exceed initial Project estimates.

The full report may be obtained from the City Auditor's website: http://www.talgov.com/transparency/auditing-auditreports.aspx. For more information, contact us by e-mail at auditors@talgov.com or by telephone at 850/891-8397.

WHAT WE RECOMMENDED

1. The City should establish a formal policy or procedure to govern City information technology systems operated in a cloud environment. That policy or procedure should address industry best practices.
2. The City should continue efforts to execute contract amendments that are in the best interest of the City such that the upgrade services can be resumed. Among other things, those amendments should establish a maximum price (fee) that will be paid for the remaining upgrade services. In the event those efforts are not successful, the City should develop alternative plans to timely upgrade the PeopleSoft Financials and HR systems.
3. Planning and scheduling of contractor site work on City projects should be enhanced to reduce associated vendor travel costs that are reimbursed by the City. Future contractual provisions regarding reimbursable vendor travel costs should establish maximum amounts that will be reimbursed.
4. Vendor invoices should be timely reviewed and paid, with support for amounts paid properly retained in City records. Supervisory review and approvals of those invoices should be documented.
5. City staff responsible for reviewing and approving contractor invoices should obtain complete and proper understandings of applicable contractual terms to ensure future overbillings do not occur.
6. For future projects of the nature addressed by this audit, competitive proposals from multiple vendors should be solicited and evaluated in connection with the acquisition of needed services.
7. Enhancements should be made to the City's procurement policy to help avoid perceived (or actual) conflicts of interest in the vendor selection process.
8. For future projects of the nature addressed by this audit, contracts for needed services should be structured to provide maximum amounts the City will pay for those services. Such contracts should also establish milestones, and provide for penalties when those milestones are not met.
9. For future projects of the nature addressed by this audit, contracts for needed services should require performance bonds insuring the City for the value of the contracted services. Insurance provisions should require adequate levels of proper coverage and provide for adequate protections of the City. The City's Risk Management Section should be consulted in making those determinations.
10. Management should continue efforts to reduce hosting costs.

We would like to thank staff in the City's Technology and Innovations Department and in Procurement Services for their cooperation and assistance during this audit.

Office of the City Auditor

Audit of the Cloud Migration & Upgrade to PeopleSoft Systems

Report #1706
April 7, 2017

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

This page intentionally left blank.

Copies of this audit report #1706 may be obtained from the City Auditor's website (http://www.talgov.com/transparency/auditing-auditreports.aspx), by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail, or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

Audit conducted by:
Patrick A. Cowen, CPA, CISA, CIA, Senior IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor

Table of Contents

This page intentionally left blank.

Audit of the Cloud Migration & Upgrade to PeopleSoft Systems

T. Bert Fletcher, CPA, CGMA
City Auditor

Report #1706 ***April 7, 2017***

Executive Summary

With the assistance of a contracted vendor, the City successfully migrated (transitioned) the PeopleSoft Financials and Human Resources systems to a cloud environment. For the most part, City staff followed industry best practices during the migration process. Efforts to subsequently upgrade the two City systems to current versions after the transition to a cloud environment were, however, suspended due to challenges resulting from a lack of clarity and specificity in certain contractual terms and conditions regarding roles and responsibilities of City and contractor staff. Payments made to the contracted vendors in connection with the transition to the cloud environment and subsequent upgrade efforts were generally appropriate and correct. Enhanced project planning and scheduling as well as stronger negotiation and contractual restrictions would likely have reduced those costs. Furthermore, while applicable contracts were executed with legitimate vendors for the needed services through authorized processes, it likely would have been more beneficial to the City if vendors had been selected using a direct solicitation of proposals through a competitive process. Lastly, hosting costs associated with the transition and upgrade efforts are expected to exceed initial City projections.

This audit was conducted to evaluate and report on management's efforts to transition the City's PeopleSoft Financials and Human Resources systems to a "cloud" environment and to subsequently upgrade those two major systems.

This audit was conducted to evaluate and report on management's efforts to transition the City's PeopleSoft Financials and Human Resources systems to a "cloud" environment and to subsequently upgrade those two major systems. Because this major information technology project (Project) is anticipated to take more than two years to complete, this audit is being conducted in two phases. This report covers the first phase, which is represented by the period

from the start of the Project through completion of the transition, or migration, of the two systems from an internally managed environment to a cloud environment. The second phase will address the City's remaining efforts to upgrade the two systems subsequent to the cloud migration.

Four objectives were established for this audit.

The specific audit objectives included the following:

- Determine if the vendors associated with the Project were selected in accordance with best practices and if contracts executed with those vendors were appropriate, adequate, and in the best interests of the City.
- Determine if payments to Project vendors were reasonable, appropriate, supported, properly approved, and in accordance with controlling contractual provisions.
- Identify best practices relating to cloud computing and determine if the migration of the two PeopleSoft systems to a cloud environment was conducted in accordance with those practices.
- Determine and report on the overall status of the Project, to include successes and challenges.

Vendor Selection and Related Contracts

An evaluation and analysis by the City showed retaining and upgrading the two PeopleSoft systems was the City's best option.

After determining Oracle Corporation (Oracle) would no longer support the PeopleSoft Financials and Human Resources (HR) versions used by the City, management researched industry trends and identified options. One option considered by the City was the replacement of the two PeopleSoft systems with non-PeopleSoft systems. However, evaluation by City staff showed available non-PeopleSoft systems did not have all desired functions and the anticipated implementation costs were higher than the anticipated costs of upgrading the two PeopleSoft ERP systems. Additionally, City management determined the need to train City employees in the use of new systems would further increase the costs of implementing non-PeopleSoft systems. Accordingly, management decided to retain and upgrade the two PeopleSoft systems to current versions that are supported by Oracle, and to also transition those systems to a cloud environment.

The City executed contracts with two vendors related to this Project, one with Ciber and one with CenturyLink.

The City executed contracts with Ciber, Inc. (Ciber) to assist the City in transitioning to a cloud environment and to subsequently upgrade those two systems to current versions. The City executed a contract with CenturyLink, LLC (CenturyLink) for the cloud hosting services. Those vendors were selected and applicable contracts were executed through authorized processes. However, it likely would have been more beneficial to the City if the vendors had been selected using a direct solicitation of proposals through a competitive process. Because the City did not solicit competitive proposals, the City cannot demonstrate the services were acquired under the most favorable terms and prices. Additionally, the manner in which the contract for upgrade services was structured increased the risk the City will pay more for those services. Lastly, for each of the three contracts for Project services (transition, upgrade, and cloud hosting), enhanced terms and provisions requiring insurance and liability protection would have better safeguarded the City from certain risks. Recommendations were made to help management ensure future services are acquired using competitive procurement methods, and to ensure future contracts contain appropriate terms and conditions to better protect the City's interests.

Issues were identified in regard to the vendor selection process and adequacy of contractual provisions.

Payments to Project Vendors

Payments made by the City related to this Project were generally correct. However, enhanced Project planning and scheduling likely would have reduced some of the City's costs.

As of the date of our audit tests, the City had paid Project vendors approximately $1.2 million for their services in connection with transitioning to the cloud environment and ongoing management of that environment, upgrade of the two PeopleSoft systems, and cloud hosting services. Payments by the City for those services were generally correct. However, enhanced Project planning and scheduling likely would have reduced some costs incurred by the City. Additionally, stronger negotiation and enhanced contractual restrictions regarding vendor travel costs would likely have further reduced Project costs. Also, enhanced understandings by Project staff of billing provisions within the respective contracts and the invoices submitted by the two contracted vendors would have better ensured the payments to contractors were proper and correct. Lastly, we noted better efforts are needed to ensure contractors are

paid timely, and evidence is prepared to demonstrate Project management is reviewing and authorizing invoices prior to City payment. We made recommendations to address each of these areas.

Best Practices for Transitioning to a Cloud Environment

Through research we identified 35 best practices considered applicable to the migration of the City's PeopleSoft Financials and Human Resources systems to a cloud environment. Of the 35 best practices, we considered 14 as the most critical to the successful migration of the two City ERP systems. Of the 14 more critical practices, we determined the City successfully followed and met eight practices; partially followed and met two practices; and did not follow the four remaining practices. Of the six practices not followed or only partially followed, subsequent actions and efforts were made, after the dates those practices should have been implemented, that showed the City did not suffer any adverse effects as a result of not initially following those practices.

The City generally followed industry best practices during the migration process.

In addition to the 14 critical best practices addressed above, we identified 21 other less critical practices applicable to the City's migration to and use of a cloud environment. We determined all but one of those 21 practices were followed and/or met. While the City has enacted other measures to protect and secure City data maintained in the CenturyLink-provided cloud environment, subsequent implementation of the one practice not followed/met will provide an additional measure to secure City data. Recommendations were made as appropriate.

Project Accomplishments, Challenges, and Current Status

The City working through the contracted vendors, Ciber and CenturyLink, created a reasonably secure cloud environment and successfully migrated the two PeopleSoft ERP systems to that environment.

Accomplishments. The City working through the contracted vendors, Ciber and CenturyLink, created a reasonably secure cloud environment and successfully migrated the two PeopleSoft ERP systems to that environment. City staff are now operating in that environment. Specific activities performed to achieve that success included:

- Development of primary and disaster recovery cloud environments in two separate data centers.
- Development and availability of adequate computing capacity for City operations.
- Migrating City systems and data to the cloud environment.
- Performance of appropriate testing of the two City systems within the cloud environment to ensure the systems functioned adequately.

Several activities relative to the subsequent upgrade of the two PeopleSoft systems have also been successfully completed prior to the date those efforts were suspended (as explained below under "Challenges"). Specifically, as of the date the systems were successfully migrated to the cloud environment and operational (in use by City staff), there were 21 Project tasks/deliverables that were to be completed by Ciber and/or City Project staff in regard to upgrading the two ERP systems and implementing additional system modules. We determined each of those 21 tasks/deliverables has been completed. *(Note: The City's upgrade contract with Ciber established 61 Project tasks/deliverables; the remaining 40 tasks/deliverables were due for completion subject to the successful migration. The completion of those remaining 40 tasks/deliverables will be addressed in a subsequent progress audit of the Project, conducted by our office, in the event the upgrade activities are resumed.)*

A lack of clarity and specificity in certain contractual terms and conditions, including tasks and expected roles and responsibilities of Ciber and City staff, as well as differences in interpretations of certain contractual terms and conditions, have caused confusion, communication issues, and delays in completion of subsequent Project phases.

Challenges. A lack of clarity and specificity in certain contractual terms and conditions, including tasks and expected roles and responsibilities of Ciber and City staff, as well as differences in interpretations of certain contractual terms and conditions, have caused confusion, communication issues, and delays in completion of subsequent Project phases. Based on discussions with Project management and staff and review of related records and correspondence, there have been several areas where the City and Ciber differed as to expectations regarding roles and responsibilities of both parties. For example, City management asserted that to keep the Project on schedule, City Project staff completed certain tasks that it interpreted to be the responsibility of Ciber, including

establishing the Virtual Private Network (VPN) that allows secure transmission of data between the City and the cloud host's data center. Also, Ciber initially asserted to the City that the fees for the cloud host vendor (CenturyLink) would be $18,500 monthly. However, the City subsequently determined that fee was significantly higher. Notwithstanding the City should have obtained a proper understanding of those fees before it executed the contracts and that Ciber has agreed to provide the City a credit due to the misunderstanding, this occurrence furthered management's concerns as to the adequacy of Ciber's communications with the City. Other contract interpretation differences pertain to disaster recovery terms and conditions.

Our audit shows that based on activity as of December 31, 2016, the hosting costs over the initial three-year period will likely exceed anticipated costs by approximately $327,000. Of that amount, Ciber has agreed to provide services at the end of the upgrade of the two PeopleSoft systems, valued at $276,000, at no charge to the City. Project management is currently exploring options to reduce future hosting costs. We recommend those efforts be continued.

Project Status. The City's PeopleSoft Financials and Human Resources systems were migrated to and are currently operating in a cloud environment. Accordingly, the first phase of the Project has been successfully completed. However, because of ongoing concerns regarding Ciber's provision of managed and upgrade services (see "Challenges" above), the City directed Ciber on January 10, 2017, to suspend further Project activities in regard to the upgrade of the two PeopleSoft systems. In that correspondence the City informed Ciber the upgrade services were being suspended to allow the City to develop and execute amendments to the contract that will clarify the roles and responsibilities of each party, address Project milestones, establish more clearly defined deliverables, and provide penalties in the event Ciber does not meet the established milestones or provide the required deliverables.

Because of ongoing concerns regarding Ciber's provision of managed and upgrade services, the City directed Ciber on January 10, 2017, to suspend further Project activities in regard to the upgrade of the two PeopleSoft systems.

City management indicated that it is currently working on those contract amendments, which have been proposed to Ciber for execution. Management indicated that if favorable amendments

cannot be executed, it will terminate the upgrade contract in accordance with existing contractual provisions.

We recommend the City continue efforts to develop and execute contract amendments that are in the best interests of the City. As part of those efforts, we also recommend City management consider establishing a maximum price (fee) that will be paid for the remaining services. In the event the City is not successful in negotiating appropriate contract amendments and the upgrade contract is terminated, the City should develop alternative plans to timely upgrade the two PeopleSoft ERP systems to current versions.

Acknowledgments

We would like to thank staff in the City's Technology and Innovations Department and in Procurement Services for their cooperation and assistance during this audit.

This page intentionally left blank

Audit of the Cloud Migration & Upgrade to PeopleSoft Systems

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Report #1706 ***April 7, 2017***

Objectives, Scope, and Methodology

Because this major information technology project (Project) is anticipated to take more than two years to complete, this audit is being conducted in two phases. This report covers the first phase, which is represented by the period from the start of the Project through completion of the transition, or migration, of the two systems from an internally managed environment to a cloud environment.

This audit was conducted to evaluate and report on management's efforts to transition the City's PeopleSoft Financials and Human Resources systems to a "cloud" environment and to subsequently upgrade those two major systems. Because this major information technology project (Project) is anticipated to take more than two years to complete, this audit is being conducted in two phases. This report covers the first phase, which is represented by the period from the start of the Project through completion of the transition, or migration, of the two systems from an internally managed environment to a cloud environment. The second phase will address the City's remaining efforts to upgrade the two systems subsequent to the cloud migration.

The specific audit objectives included the following:

Four specific objectives were established for this audit.

- Determine if the vendors associated with the Project were selected in accordance with best practices and if contracts executed with those vendors were appropriate, adequate, and in the best interests of the City.
- Determine if payments to Project vendors were reasonable, appropriate, supported, properly approved, and in accordance with controlling contractual provisions.
- Identify best practices relating to cloud computing and to determine if the migration of the two PeopleSoft systems to a cloud environment was conducted in accordance with those practices.
- Determine and report on the overall status of the Project, to include successes and challenges.

As previously noted, the scope of this first phase covered the start of the Project through migration of the two PeopleSoft systems to

the cloud. During this audit we reviewed selected Project management activities with an emphasis on vendor selection and contracting, contract payments and other financial activities, best practices, and contract compliance.

Audit procedures performed to meet our stated objectives included:

We conducted appropriate audit procedures to meet our objectives.

- Interviewing City and contractor management and staff to obtain a detailed understanding of the Project's purpose, goals, plans, and activities.
- Reviewing Project-related contracts and records to ascertain how vendors were selected and whether best practices were followed in regard to vendor selection and contracting activities.
- Selecting and testing a sample of Project-related expenditures.
- Researching and identifying best practices for migration to a cloud computing environment and evaluating Project activities to determine compliance with those best practices.
- Identifying key Project deliverables and reviewing related records to ascertain if they were provided by applicable contractors.
- Attending periodic Project meetings held by management and staff to help ascertain the Project's status, accomplishments and challenges.

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Project Definition and Purpose

An Enterprise Resource Planning (ERP) system is defined as a suite of computerized applications (modules) that are integrated to collect, store, manage, and interpret data from business activities. Companies that create, own, and/or sell ERP systems often improve or enhance (upgrade) those systems periodically; and, offer those upgraded system versions to customers (entities) using those systems. Customers generally must expend resources to implement the upgraded versions. Furthermore, once a newer version has been available for an extended period of time, the owner companies often stop providing ongoing customer support for the older versions. As a result, customers that do not obtain the newer versions within a defined period will no longer be able to obtain ongoing support of their older versions for a reasonable fee.

The City currently utilizes three separate PeopleSoft ERP systems. Of those three systems, one is used for financial management and accounting (PeopleSoft Financials), a second one for managing human resources activities (PeopleSoft HR), and a third one for managing customer utility activities (PeopleSoft Customer Information System, or CIS).

The City currently utilizes three separate PeopleSoft ERP systems. Of those three systems, one is used for financial management and accounting (PeopleSoft Financials), a second one for managing human resources activities (PeopleSoft Human Resources, or HR), and a third one for managing customer utility activities (PeopleSoft Customer Information System, or CIS). The Project addressed in this audit was established by management to upgrade the PeopleSoft Financials and HR systems to more current versions as created and made available by the company (Oracle Corporation) that owns those two ERP systems. Management may consider a similar upgrade of the PeopleSoft CIS system at a future time as part of a separate project.

The PeopleSoft Financials and HR systems were initially acquired and implemented by the City in 2001 and 1999, respectively.

The PeopleSoft Financials and HR systems were initially acquired and implemented by the City in 2001 and 1999, respectively. Both systems have been upgraded by the City twice since their initial implementations. The Financials system was last upgraded to the version currently being used (version 9.0) in 2009. The HR system was last upgraded by the City to the version currently in use (version 8.9) in 2006. Since those last City upgrades, Oracle Corporation (Oracle) has created and released additional upgraded versions of the two systems. The City intentionally did not

implement those subsequent upgrades for the purpose of saving City resources during the economic downturn resulting from the Great Recession. Notwithstanding that reason, because of those subsequent versions, Oracle announced it would no longer support the versions currently used by the City.

The PeopleSoft Financials and HR systems have not been upgraded in recent years.

After determining Oracle would no longer support the PeopleSoft Financials and HR versions used by the City, management researched industry trends and identified options. One option considered by the City was the replacement of the two PeopleSoft systems with non-PeopleSoft systems. The two non-PeopleSoft systems given significant consideration were "Workday" and "Fusion." However, evaluation by City staff showed those non-PeopleSoft systems did not have all desired functions and the anticipated implementation costs were higher than the anticipated costs of upgrading the two PeopleSoft ERP systems. Specifically, management's analysis showed the cost differential ranged from $200,000 (Fusion) to $2,200,000 (WorkDay). Additionally, City management determined the need to train City employees in the use of new systems would further increase the costs of implementing non-PeopleSoft systems. Management also reviewed the options of continuing to house and manage the systems and related data internally within the Technology and Innovations (T&I) Department, or to transition the housing and management of those systems to an external host and contracted manager (cloud environment).

Management determined the costs to replace the two PeopleSoft systems ranged from $200,000 to $2,200,000 more than the costs to retain and upgrade those two systems.

Based on the described research and evaluations, City management decided it would be more efficient and prudent to (1) migrate the City PeopleSoft Financials and HR systems to a cloud environment (external host), (2) contract with a qualified vendor to manage and oversee the cloud-hosted systems and environment, and (3) subsequent to the transition to the cloud environment, contract with a qualified vendor to upgrade the two ERP systems to the newest versions (i.e., versions 9.2 for both systems).

Management prepared an agenda item disclosing and requesting City Commission authorization for this plan. The City Commission

Authorization was provided in December 2014 to upgrade and migrate the two PeopleSoft systems to a cloud environment.

authorization was provided in its scheduled December 10, 2014, public meeting. As requested in the agenda item, that authorization provided for City management to (1) execute a contract with a cloud service provider to host the two ERP systems; (2) execute a contract with a managed services company to develop the specifications for the cloud-hosted environment, migrate the two systems to that environment, and manage that environment on behalf of the City subsequent to the migration; and (3) execute a contract with a company to upgrade the two PeopleSoft ERP systems to the newest versions and to also implement additional system modules that management deemed were needed by the City.

Cloud Computing

Cloud computing is the practice of using a facility (data center) physically located outside of an entity's internally-managed network to house (host) the entity's information technology resources, to include data and software applications.

"Cloud computing" can be defined as the practice of using a facility (data center) physically located outside of an entity's internally-managed network to house (host) the entity's information technology resources, to include data and software applications. Under this approach, the entity accesses its data and applications through an internet connection and web browser. The cloud host's data center, for purposes of this report, consists of the building and related infrastructure that house the computer servers which contain the entity's data and applications. The data center may be located anywhere: across town, in a different city, state, country, continent, etc.

An entity that elects to use a cloud environment pays the cloud host and, if also used, a separate cloud service manager for those services. The fees are typically based on the number of staff (e.g., City staff) that access and use the data, the amount of data stored and transmitted between those users and the cloud host's data center, and the specific cloud environment and services used.

The City utilizes a public cloud environment. Under that environment multiple entities (e.g., private companies, governments, citizens) share the use of the cloud host's data center (i.e., the cloud host has multiple customers using the same data center).

There are four specific industry-defined cloud environments: private clouds, public clouds, community clouds, and hybrid clouds. For the Project addressed in this audit, the City is utilizing the public cloud environment. Under that environment multiple entities (e.g., private companies, governments, citizens) share the use of the cloud host's data center (i.e., the cloud host has multiple customers

using the same data center). Because multiple entities share the data center and related infrastructure (buildings, environmental controls, backup power supply, computer servers, etc.) the cost of using a public cloud is typically less expensive than the other cloud environments. Within a public cloud environment, virtual networks are created and used to isolate each participating entity's data and applications from the data and applications of the other participating entities (customers).

The City's cloud environment is categorized as an Infrastructure as a Service, whereby it rents servers and space within the cloud host's data center to process and manage its data.

Similar to the different cloud environments, there are different categories of cloud-based services, to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS is the service appropriate to and used by the City for the Project addressed in this audit. IaaS can be defined as the circumstance in which an entity (e.g., the City), in essence, "rents" servers and space (capacity) within a cloud host's data center to process and manage its data. The cloud host does not manage or process the entity's data. The entity (City) continues to process its data through the established internet connection and web browser.

Project Phases

To facilitate management and completion of the Project, management established three implementation phases. Those phases are described below:

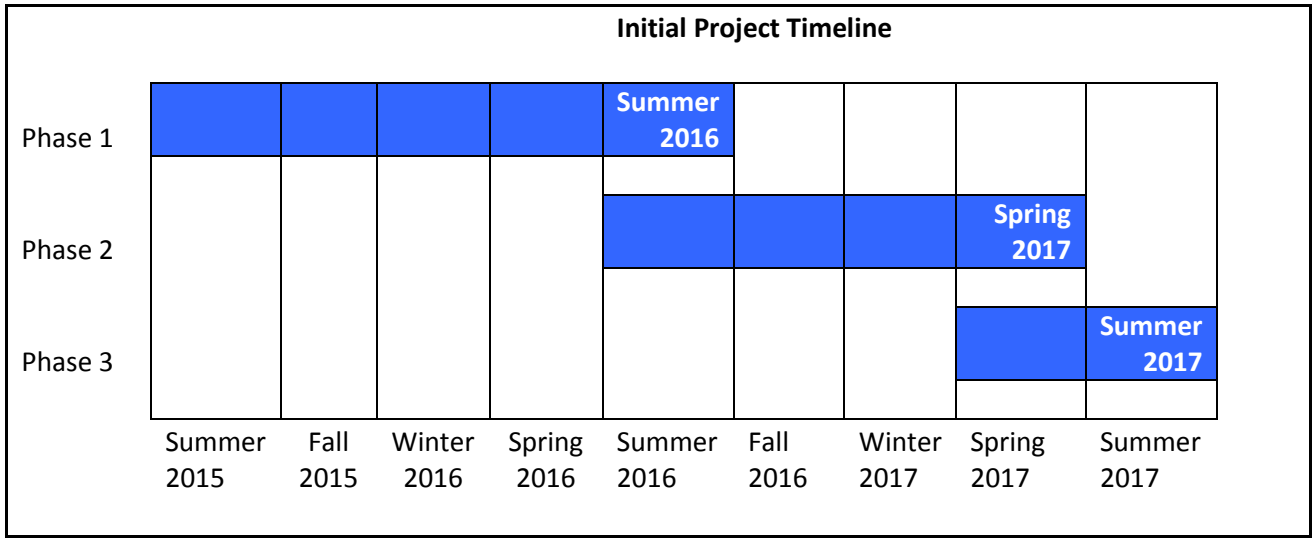
To facilitate management and completion of the Project, management established three implementation phases.

Phase 1: This phase provided for a determination of the needs and actions necessary to establish the PeopleSoft Financials and HR systems in a cloud environment, the setup and configuration of the cloud environment, and the migration from the City's internal network of those systems to that cloud environment. Management planned for this phase to be completed during the summer of 2016.

Phase 2: This phase provided for the upgrade of the City's PeopleSoft Financials and HR systems from the existing versions (9.0 and 8.9 respectively) to the most current versions available from Oracle (9.2 for both systems). Management initially planned for this phase to be completed by the spring of 2017.

Phase 3: This last phase provided for implementation of two new PeopleSoft modules and an integrated PeopleSoft application formerly not used or available to the City. The two modules were for the HR system; "ePerformance," which is an employee evaluation module, and "Enterprise Learning Management," an employee training module. The integrated application, "User Productivity Kit," is a computer–based training application to be used with both the Financials and HR systems. Management initially planned to complete this third phase in the summer of 2017.

In response to our inquiry, Project managers indicated these planned implementation and completion dates were based on projections by the vendor hired to assist the City in completing the Project. The following graph provides a representation of management's anticipated timeline for the Project.



Project Contracts

The City contracted with two entities in connection with this Project.

The City contracted with two entities in connection with this Project. One entity, Ciber, Inc. (Ciber) was hired to assist the City in each of the three Project phases and to subsequently manage the cloud-based services on an ongoing basis. The other entity, CenturyLink, LLC, (CenturyLink) was retained to provide the hosting services for the cloud environment. Additional details on

these contracted entities and the related services are provided below.

Ciber, Inc. Based on its website, Ciber is a global information technology (IT) consulting company with approximately 5,500 employees in North America, Europe, Asia, and the Pacific. The company was founded in 1974. As explained below, the City executed two separate contracts with Ciber in connection with the Project addressed by this audit.

The City executed a managed services contract with Ciber in March 2015. That contract provides for Ciber to develop the City's cloud environment, migrate the City's PeopleSoft Financials and HR system to that cloud environment, and manage and maintain that cloud environment for a 36-month term. The contract provides for a monthly fee of $21,450 for those transition (migration) and managed services. Over a 36-month period those fees will total $772,200. In accordance with management's instruction, the monthly fees were paid from Project funds through the date the migration to the cloud environment was completed and that environment was operational and in use by the City (i.e., the "cutover" date). The cutover occurred October 10, 2016. Management stated its intent is to pay monthly fees after the cutover date from operating (and not Project) funds. Although the contract was executed in March 2015, services under the managed services contract commenced in November 2015. As of the end of audit fieldwork, the City had paid a total of $278,850 in fees for services over 13 months.

The City contracted to pay Ciber $772,200 for transition and on-going managed services over a three-year period.

The City simultaneously executed a second contract with Ciber in March 2015 to upgrade the City's PeopleSoft Financials and HR systems to the new versions made available by Oracle. That second contract also provides for Ciber to implement the additional PeopleSoft modules and integrated application addressed on page 15 of this report. The upgrade services and services to implement the additional modules and application were to be provided subsequent to the cutover of the two PeopleSoft systems to the cloud environment. As explained in greater detail in a subsequent

The City also executed a contract with Ciber to upgrade the City's PeopleSoft Financials and HR systems; initial costs were estimated to be $2.4 million.

section of this report, the contract does not provide a fixed fee for the services. Instead, the contract establishes hourly billing rates for time spent by assigned Ciber staff in the provision of the applicable services. The contract also provides that related Project expenses (e.g., travel and lodging for assigned Ciber staff) will be charged to the City. The contract estimates the fees at $2,060,955 for Ciber's staff time and efforts and $334,000 for related Project expenses, for a total of $2,394,955. As of the end of audit fieldwork, the City had paid a total of $1,459,932 for those services through January 31, 2017.

Additional information on this contract and related disbursements are addressed in a subsequent report section.

The City executed an Interlocal Cooperation Contract in June 2015 with the State of Texas, which allowed the City to utilize a State of Texas contract with CenturyLink for cloud hosting services.

CenturyLink, LLC. The City executed an Interlocal Cooperation Contract in June 2015 with the State of Texas, which allowed the City to utilize ("piggyback") a State of Texas contract with CenturyLink. As authorized by that contract, the City issued a purchase order in November 2015, in the amount of $666,600 for the provision of cloud hosting services over a three-year period. Similar to the managed services contract with Ciber, expenses incurred prior to the transition of data were paid from Project funds; contract costs incurred after the transition date are to be paid from operating funds. As of the end of audit fieldwork, the City had paid CenturyLink a total of $318,123 for the cloud hosting services. This contract and related cloud hosting services are addressed in greater detail in a subsequent section of this report.

Table 1 that follows shows that status of Project contracts as of January 31, 2017.

Table 1
Status of Project Contracts as of January 31, 2017

Vendor	Contract	Contract Term	Contract Amount	Amount Paid from Project Funds	Amount Paid from Operating Funds	Total Contract Expenses
Ciber	Migration to the Cloud and Managed Services	36 months	$772,200	$235,950	$42,900	$278,850
Ciber	Upgrade of PeopleSoft ERP Systems	Until Completed *(Note 1)*	$2,394,955 *(Note 2)*	$1,459,932	Not applicable	$1,459,932
CenturyLink	Cloud Hosting	36 months	$666,600	$225,931	$92,192	$318,123
Totals			$3,833,755 *(Note 3)*	$1,921,813	$135,092	$2,056,905

Note 1: The contract amount for the upgrade of the PeopleSoft ERP systems is an estimate with the possibility of being lower or higher for the reasons explained in ISSUE #3 on pages 24 to 26 of this report.

Note 2: This amount does not address the planned credit of $276,000 that was subsequently provided by Ciber for the reasons explained in ISSUE #6 on page 28 to 31 of this report.

Note 3: Subsequent to the City Commission's authorization of funding for the Project, but prior to management's execution of the three contracts for the Project, City management determined a portion of the Migration and Managed Services and the Cloud Hosting contract costs would be paid from operating funds. Specifically, management determined that when the City began operating the Financials and HR systems in the cloud environment, the costs associated with hosting and managing those systems should be paid from operating funds and not Project funds. Accordingly, the total Project contract costs ($3,833,755) exceed the Project amount authorized by the City Commission ($3,088,400).

Audit Objective #1: Vendor Selection and Contract Execution

Overview

Competitive Acquisition of Services: As described in the background section of this report, the City selected and contracted with two separate vendors to provide services in connection with (1) the migration of the City's PeopleSoft Financials and Human Resources ERP systems to a cloud environment and subsequent ongoing management of those systems, (2) the upgrade of those systems to newer versions, and (3) implementation of two new ERP modules and an integrated training application. The first vendor, Ciber, is providing transition and ongoing managed services of the transitioned systems pursuant to one contract, and upgrade services pursuant to a second contract. The other vendor, CenturyLink, is providing the cloud hosting services under a third contract.

To ensure public funds are used (spent) efficiently, good business practices and applicable City policies and procedures provide that competitive procurement practices should be applied when appropriate in the selection of vendors to provide needed goods and services.

To ensure public funds are used (spent) efficiently, good business practices and applicable City policies and procedures provide that competitive procurement practices should be applied when appropriate in the selection of vendors to provide needed goods and services. Under competitive procurement practices (methods) the City solicits proposals from potential vendors as to the services they provide and the associated cost. The City evaluates the submitted proposals based on predetermined criteria, including price (cost), and selects the vendor with the most favorable proposal. To avoid inappropriate bias in evaluating and recommending vendors, individuals (employees) evaluating and ranking submitted vendor proposals should not have any conflicts of interests in relation to any vendors that submit proposals for consideration.

State law and City policy allows the City to utilize ("piggyback") contracts executed by other government entities.

To reduce costs associated with preparing competitive solicitations and evaluating submitted proposals, State of Florida laws and regulations and City policy and procedures allow for an alternative process. In its simplest form, that alternative process, known as "piggybacking," allows for one government entity to contract with a vendor that was previously selected by another government, generally through a competitive selection process. The contract executed by the piggybacking government would be for the same terms, conditions, and prices contained in the contract executed between the vendor and the initial (piggybacked) government.

Contracts should contain terms and conditions that properly protect the City.

Contract Terms and Conditions: Once the acquisition process for needed goods and/or services is completed, an appropriate contract should be executed with the selected vendor. The executed contract should contain terms, conditions, and provisions that protect the City's best interests. Examples include, but are not limited to, the following:

- Identification of the specific services to be provided by the vendor.
- The dates during and by which the services will be provided and completed.

- A fair and appropriate manner in which the City will be billed for the services at fees/prices established in the contract.
- Requirement for a performance bond providing restitution to the City in the event the vendor is unable to complete the provision of contracted services.
- Requirement that the vendor provides evidence of appropriate insurance coverage protecting the City in the event of damages or other adverse events.

Issues and Recommendations
Transition and Managed Services and Upgrade Services

Our audit showed competitive proposals should have been solicited, obtained, and evaluated in regard to the transition and ongoing managed services, as well as the upgrade services. Additionally, stronger and enhanced contract terms were needed in certain areas to better protect the City's interests. The specific issues and our recommendations are addressed in the following paragraphs.

Competitive proposals should have been solicited and evaluated in the selection of a contractor to perform the services related to the transition and upgrade.

ISSUE #1: Competitive proposals should have been solicited, obtained, and evaluated in the selection of a contractor to perform the transition and ongoing managed services, and upgrade services. As described previously within the background section of this report, knowledgeable City staff initially evaluated the option of replacing the two PeopleSoft ERP systems with a non-PeopleSoft system(s). That evaluation showed that implementation of new non-PeopleSoft systems would likely be more expensive and also costly in terms of training City staff in the use of those new systems. Accordingly, management decided to upgrade the existing PeopleSoft Financials and Human Resources Systems. Management also reviewed the options of continuing to house and manage the systems internally or to transition the housing and management of the systems to an external host and contracted manager (cloud environment). The decision was subsequently made that transitioning to a cloud environment should be more efficient for the City.

In response to our audit inquiries, City staff indicated that during their evaluations of available options, Oracle, the company that owns and sells PeopleSoft systems, offered the City an unsolicited proposal whereby they (Oracle) would partner with a specific IT consultant (Ciber) to transition the two City PeopleSoft systems to a cloud environment, update the transitioned (migrated) systems to new versions, implement the two new ERP modules and the integrated training application, and then manage the services on an ongoing basis. The City had previously contracted with Ciber to assist in the initial implementations of the two PeopleSoft systems (more than 10 years ago) and in assisting the City in making subsequent upgrades to those systems. Because of the City's satisfaction with Ciber in regard to those previous services and the large expense and effort anticipated with new (different) systems, City staff determined the Oracle proposal was favorable. Further, as Ciber was included as an IT vendor on an existing State of Florida (State) contract, City staff determined it could piggyback on that contract. As a result, competitive solicitations were not prepared and issued by the City, thereby saving resources and efforts and facilitating the start of the Project. Based on these circumstances, the City executed contracts with Ciber in March 2015, one contract for the upgrade services and a second contract for transition and ongoing managed services after the transition to the cloud-hosted environment was completed.

Solicitation of proposals from multiple vendors would have better ensured services were acquired at the most favorable terms and prices.

Notwithstanding the noted circumstances, the selection of and contracting with Ciber in the above-described manner did not provide for the level of competitive procurement intended by the terms and conditions of the piggybacked State contract. Specifically, the State IT consultant contract that was piggybacked includes multiple (74) vendors from which a State agency or other governmental entity can select to provide services. One of those 74 vendors is Ciber. The terms and conditions of that State contract provide that State agencies must obtain quotes from several of the included vendors when using the contract to obtain IT consultant services. The State's instructions provide that other governments (e.g., the City) are encouraged (but not required) to obtain quotes

from multiple vendors when using the contract. Contrary to that "encouragement" provision, the City contracted with Ciber without obtaining proposals from other vendors included in the State contract.

In summary the purchased transition and ongoing managed services, and upgrade services, were acquired without solicitation of competitive proposals. As a result, the City cannot demonstrate the services were acquired at the most favorable terms and price to the City. In future circumstances where services of the nature described are needed, we recommend City management ensure competitive proposals/quotes are solicited and evaluated in connection with the selection of a vendor.

Steps should be taken to ensure there are no actual or perceived conflicts of interest when City employees have formerly worked for potential contractors that are being considered for City business.

ISSUE #2: To help avoid actual and perceived conflicts of interests, the City should adopt a policy specifying the circumstances under which City employees can participate in evaluations and/or selections of proposals for City business, that are received from potential contractors for whom they previously worked. The City established an informal team of knowledgeable and experienced managers to determine and evaluate alternatives for enhancing the City's financial and human resources ERP systems (both PeopleSoft systems). As noted in the background section of this report, those systems were no longer being supported by Oracle (who owns PeopleSoft) as the City had intentionally foregone intermediate system upgrades to newer versions for the purpose of saving resources during the economic downturn that resulted from the Great Recession. The City team was comprised of staff in the following positions at the time of the evaluations:

- Director of the former Department of Management and Administration, which included the Accounting Services and Human Resources Departments.
- Chief Information Officer.
- Accounting Services Manager.
- Director of Human Resources.
- Manager, Financial Services.
- Manager, Procurement Services.

- Manager of the former Department of Budget and Policy.
- Manager, Equity and Workforce Development.

Based on the two systems being upgraded and moved to the cloud, the makeup of the evaluation team was appropriate and reasonable. However one team member, the Procurement Services Manager, was a former employee of Ciber, the vendor selected for the Project. Specifically, the Procurement Services Manager was employed by Ciber from 1991 to 2002 (11 years), at which time he left Ciber to work for the City as a financial and systems analyst for 5 and 1/2 years (i.e., from May 2002 to October 2007). In October 2007 he left the City and returned to work for Ciber until January 2012, at which time he was rehired by the City as a financial and systems analyst. He was promoted to Procurement Services Manager in October 2013. At the time (mid to late 2014) the evaluation team received and considered the Ciber proposal to transition the two City PeopleSoft systems to a cloud environment and subsequently upgrade those systems, approximately two and a half years had elapsed since his most recent Ciber employment.

Based on interviews of the various team members and review of the City Commission meeting minutes where the vendor selection was discussed and approved, the Procurement Services Manager properly did not participate in the decision process as to whether to accept Oracle's offer to partner with Ciber for the upgrade and move to the cloud. Notwithstanding those circumstances, given that (1) the Procurement Services Manager as a former Ciber employee was actively engaged as a team member in reviewing and evaluating the different alternatives for the purposes of providing information to the managers that made the decision, (2) the City did not seek competitive proposals for the services, and (3) Ciber was selected to provide the desired services, there may be a perception that a conflict of interests existed in regard to the selection of Ciber for both the transition and ongoing managed services and the upgrade services.

To help preclude future appearances of a conflict of interests in similar circumstances, we recommend the City purchasing policy be

To help avoid actual and perceived conflicts of interests, the City should adopt a policy specifying the circumstances under which City employees can participate in evaluations and/or selections of proposals for City business, that are received from potential contractors for whom they previously worked.

amended to establish the circumstances under which City employees can participate in evaluations and/or selections of proposals for City business, that are received from potential contractors for whom they previously worked. Such policy provisions should specify an appropriate length of time that must have passed, since the employee's previous employment with the potential vendor, before the employee can participate in the evaluation and/or selection process. Further, we recommend management continue with its plans to amend the City purchasing policy, based on discussions with the City's Independent Ethics Board, to require all City employees involved in the evaluation and/or selection of potential vendors for City business to complete documented and signed assertions that they are independent of, and have no conflicts of interests with respect to, the vendors evaluated and selected. City employees that do not meet the established policy requirements should not be assigned to evaluate or select proposals for the applicable City business.

ISSUE #3: The contract executed with Ciber for the upgrade services should have been structured differently to adequately reduce the City's exposure to financial risk. As described above in ISSUE #1, the City piggybacked on a State of Florida IT contract when executing a contract with Ciber for upgrade services. That State contract provides that available and selected vendors may be hired on a "project basis" or on a "staff augmentation" basis. Examples of services provided on a project basis include analysis and design, and development and integration. On the other hand, staff augmentation is to be used for services that are not project oriented. As an example, if a government needed to hire additional IT staff to provide ongoing IT services within their organization, they could contract with an included vendor (i.e., one of the 74 vendors) to provide that staff for a definite or indefinite period.

For vendors hired on a project basis, the instructions for the State contract provide the services should be acquired at a fixed price, or at a price not to exceed a specified amount.

For vendors hired on a project basis, the instructions for the State contract provide the services should be acquired at a fixed price, or at a price not to exceed a specified amount (maximum). Acquiring services under those terms has the effect of transferring the financial risk for successful completion of the applicable project

from the acquiring government entity (e.g., the City) to the contracted vendor (e.g., IT consultant). Specifically, under this approach the vendor has the financial incentive to complete the project in an expeditious manner so as to keep costs low and maximize profits.

For vendors hired using the staff augmentation approach, the acquiring government entity agrees to pay the vendor based on the time spent and value of material used by the vendor in providing the contracted services. There is no maximum amount that can be paid.

For vendors hired using the staff augmentation approach, the acquiring government entity agrees to pay the vendor based on the time spent and value of material used by the vendor in providing the contracted services. There is no maximum amount that can be paid. Under this approach, the vendor generally bills (invoices) the government entity at an hourly rate for the time vendor employees render services. Related costs such as travel and lodging are also usually billed to the government entity by the vendor. Because there is no limit as to the total amount that can be billed and paid, the financial risk for successful completion of services acquired under this approach remains with the acquiring government entity.

Because the staff augmentation approach was used, the City assumed the financial risk of ensuring timely completion of the upgrades.

While the upgrade of the PeopleSoft Systems to newer versions has characteristics of a definable "project," the City executed a contract with Ciber using the staff augmentation approach. Under the contract, Ciber has provided staff with applicable skill sets to perform tasks, defined within the contract, to accomplish the upgrades. The contract establishes the rates at which the City will be billed with rates varying based on the defined skill levels. The contract estimates those costs will total $2,060,955. The contract also estimates related costs to be billed to the City for travel and lodging will total $334,000. However, the contract states that actual costs will depend on the actual work performed and actual related costs incurred by Ciber. Accordingly, the total costs could exceed the estimates. Under these terms, the City has assumed the financial risks of ensuring the upgrades are efficiently completed.

The upgrade contract did not establish dates by which identified critical Project tasks should be completed, or penalties if those tasks (or milestones) were not timely met.

Additionally, we noted the upgrade contract did not establish dates by which identified critical Project tasks should be completed, or penalties if those tasks (or milestones) were not timely met. Establishing such milestones helps a contractor determine priorities in planning and completing a project. Furthermore, when utilizing

the staff augmentation approach the establishment of milestones, and related penalties if they are not timely met, provides a financial incentive for a contractor to ensure a project is timely completed.

We acknowledge that using the staff augmentation approach can be effective in circumstances where the City's oversight staff can reasonably control the contracted vendor's time and efforts in completing the designated tasks. We also acknowledge that (1) the City has used Ciber for similar services using this approach in the past and (2) the City has successfully used the staff augmentation approach on multiple past projects. However, because of the contractually defined tasks to be performed by the vendor and the "project" nature of the services being provided under the upgrade contract, executing an agreement using the "project" basis approach would have reduced the City's financial risks and potentially may have saved the City money. When acquiring similar services in the future, we recommend the City consider executing "project" type contracts that provide for a maximum amount the City will pay for the successful provision of contracted services. For future contracts, we also recommend the City consider establishing project milestones, and penalties when those milestones are not timely met.

Requiring the contractor to provide a performance bond for the upgrade services would have better protected the City's interest.

ISSUE #4: Requiring the contractor to provide a performance bond for the upgrade services would have better protected the City's interest. The State of Florida IT contract through which the City's contract with Ciber for upgrade services was executed (piggybacked) allows for the contracting governmental entity (e.g., State agency or other government) to require the selected vendor to furnish a performance bond. Performance bonds are instruments that insure the contracting governmental entity for the value of the contracted services in the event the vendor is unable to successfully complete its contractual tasks (due to no fault of the governmental entity). The City's contract for upgrade services did not require Ciber to obtain and provide the City such a performance bond, and no bond was provided.

While performance bonds are more common to construction contracts, they may also be required for non-construction contracts

where there is a defined set of tasks to be completed by a contracted vendor and a related end product, such as a transitioned and upgraded ERP system. Accordingly, for future contracts of this nature, we recommend the City consider requiring the contracted vendor to provide a performance bond insuring the City for the value of services to be rendered.

Stronger contractual provisions regarding insurance coverage and potential liability would have better protected the City.

ISSUE #5: Stronger contractual provisions regarding insurance coverage and potential liability would have better protected the City. Requiring contracted vendors to maintain adequate insurance coverage and to include the City as an "additional named insured" on the applicable vendor insurance policies reduces the risk the City will be liable for certain adverse incidents attributable to the vendor while providing the contracted services. Also, including terms in the contract providing that the City will not be liable for actions attributable to the contracted vendor (hold harmless provisions) better protects the City from potential financial risks.

We determined Ciber maintained liability and workers' compensation insurance coverage at the levels required by the piggybacked State of Florida contract. However, the two contracts executed by the City with Ciber did not (1) require Ciber to provide evidence the City was listed an additional named insured on the liability insurance coverage maintained by Ciber, or (2) provide that the City would be "indemnified and held harmless" for actions attributable to Ciber.

We question whether the level of liability coverage maintained by Ciber is adequate to address the risk associated with a major data breach attributable to actions (or inactions) by Ciber.

Further, we question whether the level of liability coverage maintained by Ciber is adequate to address the risk associated with a major data breach attributable to actions (or inactions) by Ciber. Specifically, in the event of a major breach where sensitive and confidential City data (e.g., employee social security numbers or addresses) is inappropriately leaked, disclosed, or stolen, we question whether the current level of liability coverage maintained by Ciber, $1 million per event or $2 million in aggregate, is sufficient.

To better protect the City, we recommend consideration be given to ensuring provisions in subsequent contracts for services are

adequate to address the above-discussed risks. Specifically, future contracts should (1) require the City be listed as an additional named insurance coverage on applicable vendor policies, (2) require the vendor to maintain adequate levels of insurance coverage, and (3) include appropriate hold harmless provisions. City staff should consult with the City's Risk Management Division in determining what levels of coverage are adequate under the circumstances.

Issues and Recommendations

Cloud Hosting Services

City management should have obtained a better understanding of the cloud hosting fees prior to executing a contract for those services. Because a proper understanding was not obtained prior to execution of the contract and commencement of services, the City is likely to pay significantly higher fees than it planned for and anticipated. Additionally, the contract executed for the cloud hosting services should have required the vendor to maintain higher levels of liability insurance coverage. The specific issues and our recommendations are addressed in the following paragraphs.

In selecting a vendor for cloud hosting services, the City did not solicit competitive proposals. Instead, the City entered into an Interlocal Cooperation Contract with the State of Texas in June 2015, which allowed the City to piggyback on an existing State of Texas contract with CenturyLink for cloud hosting services.

ISSUE #6: To help preclude Project cost overruns, City staff should obtain appropriate and complete understandings of proposed contract fee provisions prior to executing contracts. As described previously within this report, City management accepted Oracle's proposal to partner with Ciber to transition the City's PeopleSoft Financials and Human Resources systems to a cloud environment and upgrade those systems. At the time that decision was made, Ciber planned to contract directly with CenturyLink to provide the cloud hosting services. Under that initial plan, fees paid by Ciber to CenturyLink for the hosting services would be passed on to the City when Ciber invoiced the City for its services. However, the State of Florida IT contract, on which the City piggybacked to execute a contract with Ciber for transition, upgrade, and managed services, does not include cloud hosting services as one of the covered services. Accordingly, for the Project to continue with Ciber (as the vendor contracted to provide the transition and ongoing managed

services and upgrade services), it was necessary for the City to contract directly with a vendor that provided cloud hosting services.

In selecting a vendor for cloud hosting services, the City did not solicit competitive proposals. Instead, the City entered into an Interlocal Cooperation Contract with the State of Texas in June 2015, which allowed the City to piggyback on an existing State of Texas contract with CenturyLink for cloud hosting services. The State of Texas contract established pricing for the acquired services at an amount equal to "20% off the MSRP" ("Manufacturer Suggested Retail Price"). The piggybacked State of Texas contract also provides that a customer (e.g., City) may negotiate prices that are more advantageous than those provided by that contract.

Prior to contract execution, City Project staff did not obtain an adequate understanding of the pricing mechanism used by CenturyLink.

We reviewed the State of Texas contract and subsequent City purchase order issued in November 2015 to CenturyLink for the hosting services. That initial City purchase order for hosting services provided for a monthly base payment in the amount of $18,500, or a three-year (36 months) cost of $666,000. In response to our inquiry as to how the initial monthly fee of $18,500 was established, City Project staff responded that Ciber initially obtained a quote from CenturyLink on behalf of the City in the amount of $18,500 per month, and the City accepted that fee when executing the interlocal agreement and purchase order.

In June 2016, the City and CenturyLink executed an amendment (change order) to the initial agreement. The amendment provided for CenturyLink to acquire database licenses necessary to house and process the City's data and applications at CenturyLink data centers (i.e., the cloud hosted environment). The amendment increased the monthly service fee from a base of $18,500 to $21,279, a monthly increase of $2,779. As explained by City Project staff, the City would have incurred those costs regardless of the amendment, as the City would have purchased those database licenses from the vendor (Microsoft) for use by CenturyLink if they had not provided the funds for CenturyLink to instead acquire the licenses directly from Microsoft.

After executing the purchase order with CenturyLink and commencement of cloud hosting services, City staff indicated a determination was made by Ciber and City Project staff that, based on the actual pricing mechanism used by CenturyLink, the actual monthly costs would often exceed the base fee.

After executing the purchase order with CenturyLink and commencement of cloud hosting services, City staff indicated a determination was made by Ciber and City Project staff that, based on the actual pricing mechanism used by CenturyLink, the actual monthly costs would often exceed the base fee (initially $18,500 and later revised to $21,279). Specifically, based on CenturyLink's pricing mechanism, the $18,500 (revised to $21,279) actually represents a minimum monthly fee. In the event the value of the monthly usage of hosting resources exceeds the minimum monthly fee, the City will pay the value of that actual usage, reduced by a factor of 20%. The value of the "usage" equates to the "MSRP" as contained in the State of Texas contract. Our review of the CenturyLink invoices paid by the City for the initial seven months of hosting services (November 2015 through May 2016) confirmed this billing process, as the City paid the minimum monthly fee when the value of the usage was less than that minimum fee, and paid more than the minimum monthly fee for the one month where the value of the usage (discounted by 20%) exceeded the monthly minimum fee. As future monthly usage was anticipated to increase, the City is expected to continue to pay monthly fees greater than the current minimum fee of $21,279. Specifically, based on estimates obtained by Project staff, the monthly fee is expected to be $7,000 to $9,000 more than the amounts initially anticipated and budgeted. For the initial 36-month period of services, that expected increase totaled $276,000.

Because of the miscommunication regarding CenturyLink's fee, Ciber agreed to a change order whereby the City would not be billed for hours worked by Ciber staff on the Project valued at $276,000.

As Ciber had initially advised the City on this matter, Ciber agreed to offset the estimated increased cost (fees) through a change order to its contract with the City for upgrading the Financials and HR systems. Accordingly, the City and Ciber executed a change order in December 2015 that provided for Ciber not to bill the City for hours from Ciber staff to make up the $276,000, at the end of the upgrade Project.

The above-described circumstances are indicative of inadequate Project planning and oversight. Specifically, the purchase order with CenturyLink was executed with City staff not having a complete understanding of the manner and basis on which the City

would be billed for hosting services. As a result, the cost of the hosting services is significantly higher than what the City planned and anticipated. Because the City relied on information and advice from Ciber when contracting with CenturyLink, the City was successful in negotiating a change order (with Ciber) that may allow the City to recoup a portion of the higher than anticipated cloud hosting costs. Had Ciber been unwilling to execute the change order, the City would have been contractually bound to incur those costs. In future similar circumstances, we recommend City project management, prior to execution of contracts, obtain a complete and proper understanding of the vendor's billing processes to allow for an accurate estimation of associated project costs, and a basis to determine if those costs are reasonable and competitive. If City Project staff had taken these recommended actions prior to entering into the interlocal agreement, they would have had the opportunity to attempt to negotiate more favorable prices as allowed by the State of Texas contract.

It would have been to the City's benefit to solicit competitive proposals for the needed hosting services once it was determined that the City would acquire those services directly.

Furthermore, we acknowledge that piggybacking off another government's contract is an allowed practice, and those contracts are generally awarded based on competitive procurement practices. Notwithstanding those circumstances, we believe it would have been to the City's benefit to solicit competitive proposals (quotes) for the needed hosting services once it was determined the City would acquire those services directly. The intent of competitive procurement practices is to help ensure the purchasing entity acquires the best goods/services at the most favorable prices. If the City had solicited competitive proposals, it may have obtained pricing more favorable than that obtained through the State of Texas contract. Accordingly, in future circumstances of this nature, we also recommend the City solicit competitive proposals. Such proposals should be compared to those prices available on existing government contracts, and the entity with the best proposal and/or prices selected to provide the needed services.

Stronger contractual provisions regarding insurance coverage and potential liability would have better ensured the City was adequately protected.

ISSUE #7: Stronger contractual provisions regarding the level of insurance coverage were needed to adequately protect the City from risks associated with data breaches. Requiring contracted vendors to

maintain adequate insurance coverage reduces the risk the City will be liable for certain adverse incidents attributable to the vendor while providing the contracted services. We determined CenturyLink maintained liability and workers' compensation insurance coverage. However, in the course of our audit work there were questions as to whether the required and certified level of liability coverage maintained by CenturyLink was adequate to address the risk associated with a major data breach attributable to actions (or inactions) by CenturyLink. Specifically, in the event sensitive and confidential City data (e.g., employee social security numbers or addresses) is inappropriately leaked, disclosed, or stolen, it was not clear if the coverage levels communicated to the City as being maintained by CenturyLink, $1 million per event or $2 million in aggregate, was sufficient. As the result of our concerns, we met and consulted with the City Treasurer-Clerk's Risk Management Division on this matter. Through their efforts made as a result of our inquiry, a determination was made that CenturyLink does maintain adequate levels of insurance coverage. Specifically, evidence was obtained that liability insurance was maintained in amounts that provide coverage up to $3 million per event and $15 million in aggregate. Notwithstanding this subsequent determination made as a result of our audit inquiry, the City's contract with CenturyLink did not include provisions requiring adequate liability insurance coverage.

A determination was made in response to our inquiry that CenturyLink maintained adequate liability coverage.

To better protect the City, we recommend consideration be given to ensuring provisions in subsequent contracts for services are adequate to reduce the City's exposure to liability. Specifically, future contracts should require the vendor to maintain adequate levels of insurance coverage. City staff should consult with the City's Risk Management Division in determining what levels of coverage are adequate under the circumstances prior to the execution of those contracts.

Consideration should be given to ensuring provisions in subsequent contracts for services are adequate to reduce the City's exposure to liability; the City's Risk Management Division should be consulted in those matters.

Conclusion

While contracts were executed with legitimate vendors for the needed Project services through authorized processes, the vendors should have instead been selected through a process whereby the City would directly solicit competitive proposals from potential vendors, evaluate the submitted proposals, and select the vendor with the most favorable proposal. Because that competitive process was not used, the City cannot demonstrate the services were acquired under the most favorable terms and prices. Additionally, the contract for upgrade services was structured in a manner that increased the risk the City will pay relatively higher fees for those services. Lastly, for each of the three contracts for services, enhanced terms and provisions requiring insurance and liability protection would have better safeguarded the City from certain risks. We provided City management recommendations to ensure similar issues do not occur in future contracts for services.

Audit Objective #2: Project Expenditures

Payments made by the City to Ciber and CenturyLink were tested to determine if the associated charges were reasonable and appropriate, correctly calculated, in accordance with contractual provisions, adequately supported, and approved by authorized City Project staff.

Overview

As explained in the following paragraphs, this audit objective covered payments made by the City to two contractors, Ciber and CenturyLink.

Ciber: For purposes of this audit, we identified and tested payments made by the City to Ciber pursuant to the managed services contract and the upgrade contract. Our population included payments made from the beginning of Ciber's involvement in the Project (April 2015) through June 2016, and was comprised of eight payments totaling $1,195,095. Those eight payments represented 45 Ciber invoices (multiple invoices were accumulated and paid in the aggregate). Each payment and invoice was tested. The services represented by those payments are shown on the following table.

Table 2 **Payments to Ciber through June 2016**		
Contract	Services	Total Payments
Upgrade Services	Ciber Staff Time on Project	$1,000,660
Upgrade Services	Ciber Staff Travel & Lodging	$65,735
Transition & Managed Services	Ongoing System Management	$128,700
TOTAL		**$1,195,095**

Each payment was tested to determine if the associated charges were reasonable and appropriate, correctly calculated, in accordance with contractual provisions, adequately supported, and approved by authorized City Project staff. Analyzing payments for Ciber staff time spent working on the Project included verifying time sheets were provided substantiating the employees and time worked, and the hourly rates charged were in accordance with the contract rates established for the skill sets applicable to the employees. For travel and lodging charges, our test criteria included verifying employee time sheets supported the period covered by the travel, there were appropriate receipts (hotel, airfare, taxi, etc.) substantiating the charges, and the charges were not greater than those allowed by City travel policy.

CenturyLink: We tested payments by the City to CenturyLink for cloud hosting services. At the time of our fieldwork in this area during August 2016, the City had made six payments covering eight monthly invoices (one payment was for three months). Those payments totaled $160,141. Each payment and invoice was tested to determine if the related charges were reasonable and appropriate, correctly calculated, in accordance with contractual provisions, adequately supported, and timely reviewed and approved by authorized City Project staff.

Issues and Recommendations

Payments to Ciber

Ciber invoices were not always timely processed and paid by the City.

Overall, the 45 tested invoices show that charges invoiced and paid by the City to Ciber were reasonable, appropriate, adequately supported, in accordance with governing contractual provisions, and properly authorized and approved. However, instances were noted where enhancements and improvements were needed regarding reviews by City staff prior to payment. Specifically:

- The City's prompt payment policy provides that vendor invoices should be paid within 45 days of the City's receipt of a proper invoice. Of the 45 invoices, 29 were paid more than 45 days after the date the City received the invoices from Ciber. While the dates the invoices were received by the City were not documented, the period between the dates of the invoices and the dates of payment for those 29 invoices ranged from 51 days to 227 days. The delays were attributed to the Project and Technology and Innovation (T&I) administrative staff not timely reviewing and approving the invoices before submitting those invoices to the City Accounts Payable Section for final processing and payment.

City management's review and approval of Ciber invoices were not always documented.

- While the invoices were reviewed and approved, those approvals were not always adequately documented. For 23 of the 45 invoices, there was no documentation showing appropriate T&I management had approved the invoices. Documentation of supervisory review is necessary to clearly demonstrate determinations were made as to the propriety and appropriateness of payments.

Adequate support was not available to support and substantiate some costs.

- Adequate support was not available to support and substantiate all or some costs shown on 9 of the 45 invoices. For those items the City requested and obtained the necessary documentation (supporting employee time sheets and vendor receipts substantiating travel costs) from Ciber in response to our audit request. In those instances, current T&I staff indicated the support likely was available at the time the invoices were reviewed and approved, but that support may have been

misplaced and not properly filed or entered into the City's records management system during transitional changes that occurred when the former Information System Services department was reorganized into the T&I Department, and when key administrative responsibilities were being transferred as certain staff retired or were reassigned.

- Ciber obtained airline tickets for their Project staff to travel to and from Tallahassee to work on the transition to the cloud and systems upgrades. In our review we noted the following:

  – Five instances where Ciber acquired airline tickets for named Ciber employees with specific departure dates, but the departure dates were subsequently changed to a later date. In each of those instances the airlines charged Ciber an exchange fee (generally $205) for the change in departure dates. There were no documented explanations as to why the City reimbursed Ciber for the exchange fees, which totaled $1,264. In response to our inquiry on these items, T&I Project management indicated these instances were each attributable to the City requesting Ciber to reschedule their planned onsite reviews because City management needed to change priorities for City staff. These changes in priorities cost the City $1,264.

Airline ticket exchange fees were reimbursed by the City when City management requested Ciber to reschedule their planned onsite reviews.

  – Three instances where Ciber invoiced and the City paid charges for airline tickets for which there was no evidence the tickets were used by Ciber employees to fly to Tallahassee to work on the Project. The costs of those unused tickets totaled $2,012. In response to our inquiries on this matter, both City Project staff and Ciber representatives acknowledged the unused airline tickets. They indicated the tickets had been acquired in advance by Ciber based on dates the City Project staff had scheduled Ciber staff to be onsite for Project work. However, when City Project management rescheduled that work due to other priorities (see previous item), those tickets went unused. These changes in priorities cost the City $2,012.

The City reimbursed Ciber for the costs of unused airline tickets when City management rescheduled onsite work due to other City priorities.

In four instances Ciber invoiced and the City paid for round trip flights for Ciber employees working on the Project in Tallahassee to fly home for the weekend and then return to Tallahassee the following work week.

- Four instances where Ciber invoiced and the City paid for round trip flights for Ciber employees working on the Project in Tallahassee to fly home for the weekend and then return to Tallahassee the following work week. In each of those instances it would have been less expensive for the employees to have stayed in Tallahassee over the applicable weekend. The costs for the four round-trip tickets exceeded the associated extra lodging and meal costs (incurred if the employees had stayed in Tallahassee) by $2,129. In response to our inquiry on this matter, Project management indicated that while T&I did negotiate rates and travel costs with vendors during the contracting process, such negotiations did not address specific terms regarding amounts the vendor would be reimbursed for vendor employees working onsite (at the City) but traveling home on weekends.

A few Ciber employees stayed in more expensive hotels.

- Three instances were noted where Ciber employees stayed in hotels or rooms that were more expensive than the hotel or rooms used by other Ciber employees, and the costs of those more expensive hotels/rooms were invoiced to and paid by the City. Furthermore, because the more expensive hotels were not in close proximity to City Hall, the applicable Ciber employees incurred additional transportation costs (rental car and related parking) that were also invoiced to and paid by the City. The incremental costs paid by the City for these three instances totaled approximately $1,399. In response to our inquiry on this matter, Ciber representatives indicated the applicable traveling individuals stayed at an alternate hotel when the other less expensive hotel, used by other Ciber employees, did not have a sufficient number of rooms available for all Ciber employees.

Recommendations were made to help preclude future instances and to help lower costs on future City projects.

In summary, our testing identified charges that were not always paid timely and adequately supported (i.e., prior to our inquiry). Evidence of Project management approval also was not always documented. Additionally, we identified some "excess" (unnecessary) charges totaling $6,804, some of which likely could have been avoided through enhanced procedures and better

planning by City management. To help preclude future instances of the nature described and to help lower Project costs, we recommend the following:

- Actions should be taken to require timely review and approval of invoices by Project and designated T&I administrative staff. Furthermore, the actual dates of receipt of each subsequent invoice by T&I should be documented (e.g., by a date stamp).
- Supervisory approval of each invoice should be properly and adequately documented.
- Support for each charge and payment should be retained.
- Efforts should be made by management to better plan Project work priorities and schedule onsite work by contracted employees.
- T&I should develop practices to negotiate maximum amounts that will be reimbursed for travel costs incurred when vendor employees travel home on weekends between work weeks spent onsite at City (of Tallahassee) locations.
- T&I should develop practices to negotiate maximum amounts that will be reimbursed for travel costs incurred in future projects of this nature.

Issues and Recommendations
Payments to CenturyLink

While the amounts invoiced by CenturyLink and paid by the City for the first eight months of services were generally proper, an overbilling did occur.

Overall, the amounts invoiced by CenturyLink and paid by the City for the first eight months of services, totaling $160,141, were proper, reasonable, appropriate, and in accordance with contractual provisions. However, we determined T&I Project staff did not obtain an adequate understanding of the contract billing provisions and was paying amounts billed by CenturyLink without verifying the reasoning and logic of the invoiced amounts, thereby increasing the risk the City was not paying appropriate amounts for hosting services. For the first eight monthly payments, those circumstances resulted in Project staff not detecting one overbilling in an amount of $5,123, resulting in an overpayment by the City in that amount.

Our review also showed the City incorrectly received credits for certain taxes which the City had properly not paid (i.e., those taxes were not applicable and were correctly not assessed on City charges). Those credits were received in three of the eight months reviewed and totaled $511. Lastly, based on our inquiries, we found that CenturyLink charged the City late fees totaling $906, for which CenturyLink indicated it did not intend to assess. Upon our identification of the overpayments and incorrect charges, CenturyLink credited the City for $6,029 (comprised of the $5,123 overcharge and $906 in un-intended late fees, CenturyLink elected not to request reimbursement for the $511 incorrectly credited to the City). We recommend T&I and other Project staff assigned responsibility for reviewing and approving CenturyLink invoices obtain a complete and proper understanding of applicable contractual terms and related billing processes. That understanding should be used to ensure future amounts billed are proper, reasonable, and appropriate.

To avoid future overpayments, City staff assigned responsibility for reviewing and approving CenturyLink invoices should obtain a complete and proper understanding of applicable contractual terms and related billing processes.

Additionally, similar to two of the issues identified previously for Ciber payments, we noted the following:

- Two invoices were not paid timely by the City due to delays by T&I Project staff in determining the proper funds from which to pay the invoiced amounts. Notwithstanding that CenturyLink elected not to charge the City for late payments, the City should pay its invoices timely.
- The T&I Project manager reviewed and approved each invoice; however, that approval was not documented on five of the eight monthly invoices paid to date. Such approval should be documented.

Conclusion

Payments by the City for contractual services were generally correct. However, enhanced Project planning and scheduling likely would have reduced some costs incurred by the City. Additionally, stronger negotiation and enhanced contractual restrictions regarding vendor travel costs also would likely have reduced Project costs.

Further, enhanced understandings by Project staff of billing provisions within the respective contracts and the invoices submitted by the two contracted vendors would have better ensured the payments to contractors were proper and correct. We also noted better efforts are needed to ensure contractors are paid timely, and evidence is prepared to demonstrate Project management is reviewing and authorizing invoices prior to City payment. We made recommendations to address each of these areas.

Audit Objective #3: Best Practices

Overview

Our third audit objective addressed whether the City followed best practices in migrating the two PeopleSoft ERP systems to a cloud environment. In identifying best practices for this audit objective we researched and reviewed information technology and audit reports of other entities, authoritative guides and reports (i.e., white papers), periodicals, and other industry materials[1]. Additionally, we considered practices identified through prior audit experience. Topics addressed by the identified best practices include data and/or system security, privacy, protection, and access; environmental controls; backup and disaster recovery; and system performance and availability. Through our research we identified 35 best practices considered applicable to the migration of the two systems. Of the 35 best practices, we considered 14 as the most critical to the successful migration of the two City ERP systems.

---

[1] Examples of sources for best practices include:

1. Halpert, Ben. (2011). *Auditing Cloud Computing: A Security and Privacy Guide*. Hoboken, NJ: John Wiley & Sons.
2. KPMG, International. (2013). *Assessing the Audit Impact of Cloud Computing*.
3. Cloud Standards Customer Council. (2015, March). *Security for Cloud Computing: 10 Steps to Ensure Success*.
4. County of San Diego, California. (2015, March). *Cloud Computing Audit* (Report number A14-034). San Diego, California.
5. Chenxi, Wang, PhD. (2009, October 30). *Cloud Computing Checklist: How Secure is Your Cloud?*. Forrester Research, Inc.
6. eSentire Managed Security Services. (2012, November). *Cloud Based Security Checklist.*
7. Vogel, Dominic. (2013, March 11). *Ask Potential Cloud Vendors These 10 Security Questions.* Tech Republic.

Issues and Recommendations

Thirty-five best practices for transitioning to a cloud environment were identified; 14 of those 35 were considered the most critical.

Of the 14 more critical practices applicable to the City's migration to the cloud environment, we determined the City successfully followed and met eight practices; partially followed and met two practices; and did not follow the four remaining practices. Of the six practices not followed or only partially followed, subsequent actions and efforts were made, after the dates those practices should have been implemented, that disclosed the City did not suffer any adverse effects as a result of not following those practices. The 14 best practices and the status of our audit determinations as to compliance are described in the following table.

Table 3
Critical Best Practices: Migration to a Cloud Environment

Critical Best Practice	Actions Taken and Status
1. A Business Continuity/Disaster Recovery Plan (DR Plan) should be developed for the cloud environment.	✓ City staff worked with Ciber, as part of the managed services contract, to develop and test a DR Plan to help ensure business continuity in the event of a disaster that disrupts the City's use of the Financials or HR systems in the cloud environment. Specifically, the DR Plan provides for: • Definition of what constitutes a disaster. • Disaster recovery response times. • A strategy for recovery/restoration of the Financials and HR systems. • Testing of the DR Plan, including testing the recovered/restored Financials and HR systems. Based on the existence and substance of the DR Plan for the cloud environment, we consider this best practice to have been met.
2. Data ownership should be stipulated in contracts with cloud hosting service providers.	✓ The contract with CenturyLink includes language stating the data, materials, and intellectual property rights hosted in CenturyLink data centers are owned by the City. Accordingly, we consider this best practice to have been met.
3. A cloud environment (e.g., servers, network infrastructure, communication capacity, etc.) should be tested extensively prior to transitioning to that cloud environment. Such testing should include key users completing actions they normally would perform in the course of their work for the purpose of ensuring those tasks can be accomplished appropriately.	✓ City staff performed appropriate testing of the Financials and HR systems in the cloud environment. This included the conducting of User Acceptance Testing (UAT) on both the Financials and HR systems prior to the systems being made available for use by City staff. UAT is a comprehensive test where key users from City departments perform their daily, monthly, or annual processes in the cloud environment to identify issues that need to be addressed and corrected before that environment becomes fully operational for use by City staff.

	UAT tests included, but were not limited to, simulating the processing of payroll, hiring new employees, and preparation of financial statements. However, the City did not perform load testing to ensure the cloud environment was adequate to meet the volume of activity expected during normal City operations. In spite of the lack of load testing, the City has not experienced any slowdowns or interruptions of the Financials or HR systems in the cloud environment (through the end of our fieldwork). Accordingly, we consider this best practice to have been met. Nevertheless, we recommend in future cloud migrations that load testing be conducted as appropriate.
4. Data in the cloud should be backed up and protected in accordance with organizational standards.	✓ Pursuant to contractual terms, Ciber is responsible for establishing the backup and recovery process for the City's data in the cloud environment. As part of the Project, a back-up data center was identified and committed for this purpose. To ensure City data is protected from loss, it is mirrored (i.e., copied or backed-up) to the backup data center hourly. This method of backing up City data exceeds data back-up standards as established in City Administrative Procedure #809.5.9.1.7. As such, this best practice is considered to have been met.
5. Appropriate measures should be taken to prevent unauthorized intrusion and malware in cloud based data centers	✓ CenturyLink (the City's cloud provider) has implemented an Intrusion Prevention System (IPS) to protect the data centers used by the City (i.e., primary and back-up data centers). An IPS is an application that is installed in a network or data center to detect unauthorized intrusions and take measures to prevent those attempts from harming the network, data center, or data contained therein. City management stated that in addition to the IPS provided by CenturyLink for the data centers housing City data, the City has established firewalls and malware protection for the City's cloud environment. Accordingly, we consider this best practice to have been met.
6. Cloud service providers should, on a regular and periodic basis, conduct (or have conducted) testing of the security of their data centers. Such tests should include, at a minimum, vulnerability scans and network penetration testing. Appropriate action should be taken based on the results of those scans and tests.	✓ CenturyLink hires a third party to periodically perform vulnerability scans and penetration tests of their cloud infrastructure, including the two specific data centers housing City data. The results of the scans and tests as well as actions taken in response to the results of those scans and tests are communicated to the City as part of independent IT security audits of CenturyLink's data centers. Those audits are conducted in accordance with American Institute of Certified Public Accountants (AICPA) standards. Accordingly, we consider this best practice to have been met.
7. Contracts for cloud services (e.g., data storage and application hosting) should include service level agreements (SLAs) that address cloud availability.	✓ The Service Level Agreement (SLA) between the City and CenturyLink establishes availability standards, and provides financial penalties in the event those availability standards are not met. Specifically, CenturyLink guarantees the individual servers housing City data will be available 99.99% of the time. Accordingly, we consider this best practice to have been met.

8. Organizations should ensure data hosted in a cloud environment is stored in data centers physically located within the contiguous United Sates.	✓ Because laws of other countries that govern data security and privacy may not be as restrictive or appropriate as United States (U.S.) laws, cloud providers' data centers should be housed (located) within the United States. Furthermore, it is preferable that the cloud providers' data centers for the City be housed within the contiguous forty-eight states, as data transmitted to and from Alaska or Hawaii must cross another country or international waters, thereby increasing the risk that U.S. laws may not protect data during transmissions. The City's contract with CenturyLink enables the City or Ciber, as the City's contracted managed services vendor, to select the data centers in which City data will be maintained. Accordingly, the City has the ability to restrict the location of data centers maintaining City data to the contiguous United States. The primary and backup data centers used by CenturyLink to maintain City data are located in the contiguous United States. As a result, this best practice has been met.
9. A formal plan should be established to provide a smooth transition when cloud based applications and data are transitioned from one cloud service provider to another, or transitioned (back) to an "in-house" (internal) environment.	❖ City management reported a formal plan for transitioning the Financials and HR systems from the current cloud service provider to another cloud provider (or back to the City) will not be established until a determination is made that such a transition will occur. City staff stated partial informal plans related to the mechanism for the relocation of City data to a different cloud hosting site had been developed. Specifically, data transfers to a different data center (or back to the City) would be performed through a Virtual Private Network (VPN) connection between CenturyLink and the other data center (e.g., another cloud service provider). A VPN is an encrypted private "tunnel" established between two networks. Additionally, City management stated preliminary discussions had been held as to where City data should be submitted (transferred) in the event of the sudden or unanticipated need to depart the CenturyLink cloud environment. Based on the actions taken by management to prepare for a transition from the current cloud service provider, we consider this best practice to have been partially met. Nevertheless, we recommend management continue working towards developing and documenting a formal plan to guide staff in the event the City leaves the current cloud service provider.

10. To protect its integrity, data in a cloud environment should be encrypted at all times (i.e., while stored in a data center and while being transmitted to and from the data center).	❖ City data is encrypted during transmission between City users and the cloud host's (CenturyLink) data center. Specifically, City data is transmitted to and from the CenturyLink's data center through a VPN, which, as previously noted, provides for encryption of data during transmission. However, City data maintained at CenturyLink's data center is not encrypted when not being transmitted. That lack of encryption when the data is not in use may increase the risk of inappropriate or unauthorized disclosure of that data. In response to our inquiry on this matter, City management indicated an evaluation was currently being done to determine if further encryption of data (i.e., while not in transmission) will negatively impact the performance of the PeopleSoft Financials and HR systems. If performance (use by the City) is not negatively impacted, City management will consider further encryption. Based on the above circumstances, we consider this best practice to have been partially met. We recommend management complete its evaluation to determine the impact further encryption may have on the performance of the Financials and HR systems, and take appropriate actions based on the results of that evaluation.
11. Organizations should know who has administrative level access to data and applications in their cloud environments.	♦ Currently, the City does not have knowledge as to the individuals that Ciber, as the vendor hired to manage the City's cloud environment and upgrade the two City ERP systems, has provided administrative access to City data and applications. Specifically, based on the current configuration of the City's cloud environment as designed and implemented by Ciber, the City does not have the capability (i.e., appropriate level of access) to independently identify Ciber or other non-City staff, such as Ciber subcontractors, that have been granted access to City data and applications by Ciber. Knowledge of the individuals granted access by Ciber allows the City to ensure inappropriate or unnecessary access is not granted. Additionally, City Administrative Policy and Procedure (APP) 809, which addresses City Information Systems Security, requires non-City parties (e.g., vendors or contractors) to complete a "Compliance Statement" before they will be granted access to City's IT resources and related data. In completing the Compliance Statements those individuals attest they understand and agree to abide by City policies and procedures regarding City IT resources and data. We acknowledge that APP 809 provides these requirements are applicable to the City's internal networks and that the data maintained at CenturyLink's cloud environment represents an external network. Notwithstanding this condition, it is appropriate that, in the absence of formal City policies and procedures for cloud environments, the City

	should require similar attestations for individuals accessing City data in a cloud environment. Based on the above-described circumstances, we consider this best practice as not met. We recommend the City obtain from Ciber a system access that allows designated City staff to determine individuals granted access by Ciber to City IT resources and data. We also recommend the City require those non-City individuals granted access to City IT resources and data to attest they will abide by appropriate City policies and procedures.
12. Prior to the selection of a cloud vendor (host), organizations should obtain and review appropriate independent IT security audit reports based on standards set forth by the American Institute of Public Accountants (AICPA). Appropriate actions should be taken based on the information identified in the audit report.	♦ As part of this audit we requested from City management copies of independent IT security audit reports addressing the cloud service provided by CenturyLink and its data centers hosting City data. At the time of our request, copies of those audit reports had not been obtained or reviewed by the City. Accordingly, this best practice was not met. Subsequent to our request, CenturyLink provided copies of the applicable audit reports. Our and City management's reviews of those audit reports did not identify any issues which indicated the City's data was not adequately secured. In conclusion, while the applicable IT security audit reports were obtained and reviewed, those audit reports were not obtained prior to City data being transferred to the cloud environment thereby creating uncertainty as to the security of that data. To help ensure City data will be reasonably protected, we recommend appropriate independent IT security audit reports be obtained and reviewed prior to the selection of future cloud vendors and their data centers in which City data will be maintained.
13. An organization's risk management team should be consulted prior to executing a contract with a vendor to review and determine if the proposed vendor's insurance coverage is adequate given the types of risk associated with the particular cloud service being acquired.	♦ As noted within a previous section of this report, the City's Risk Management Division determined, at our request, that CenturyLink's coverage is adequate given the risk of migration of confidential personnel data to the cloud. However, City Project staff did not consult with Risk Management or otherwise determine the adequacy of insurance coverage prior to the execution of the contract with CenturyLink. Accordingly, this best practice was not met. We recommend applicable City staff consult with Risk Management as to the adequacy of insurance coverage prior to the execution of future contracts for cloud service.

14. Organizations should have and follow a formal and documented cloud policy when conducting IT operations in a cloud environment.	♦ The City has not created a formal policy or administrative procedure to govern City IT operations in a cloud environment. Management has expressed their intent to establish such a policy. Because a policy or procedure has not yet been established, this best practice has not been met. We recommend the City follow through on intentions to create and put into practice a comprehensive City Administrative Policy and Procedure addressing cloud computing.
Table Legend:	✓ Denotes the best practice was followed ❖ Denotes the best practice was partially followed ♦ Denotes the best practice was not followed

Twenty of the 21 "less critical" best practices applicable to migration and use of a cloud environment were met.

In addition to the 14 critical best practices addressed above, we identified 21 other less critical practices applicable to the City's migration to and use of a cloud environment. Those 21 additional best practices are shown in Appendix A to this report. We determined all but one of those 21 practices were followed and/or met. The one practice not followed or met pertains to the utilization of "geo-blocking" as an additional measure to ensure security of City data maintained in a cloud environment. Geo-blocking involves the practice of limiting remote access to an IT system and related data through tools that preclude remote computers located outside of a defined geographical area from accessing a system and its data. As an example, geo-blocking could be used to preclude computers (i.e., IP addresses) outside the United States from accessing a system and its data. While the City has enacted other measures to protect and secure City data maintained in the CenturyLink-provided cloud environment, we recommend City management consider implementation of geo-blocking measures to further limit unauthorized access to City data stored in the PeopleSoft Financials and HR systems.

Conclusion

Overall, the City followed and met industry best practices for migration of City systems and data to a cloud environment. For those best practices not met or only partially met, the City has not suffered any identified adverse consequences. Further, actions were taken after our audit inquires and discussions with Project staff on some of these practices such that the City subsequently achieved

compliance with those practices. Recommendations were made as appropriate.

Audit Objective #4: Project Status and Successes and Challenges

Overview

Our last audit objective was to determine and report on the status of the Project as of the end of our audit fieldwork in January 2017. As described in the background section of this report, there are three distinct phases for this Project (1) developing a cloud environment and transitioning the City's PeopleSoft Financials and HR systems to that environment, (2) upgrading those two PeopleSoft systems to the most current available versions subsequent to the transition to the cloud environment, and (3) implementing two new PeopleSoft modules and an integrated training application determined appropriate for City operations. While the first phase has been successfully completed, challenges have arisen that have, at least temporarily, halted the second and third phases of the Project. Specific information on the accomplishments and challenges, as well as the Project's current status, is provided in the following paragraphs.

The City successfully migrated the two PeopleSoft ERP systems to the cloud environment.

Project Accomplishments and Successes

Phase 1 was successfully completed. The City working through the contracted vendors, Ciber and CenturyLink, created a reasonably secure cloud environment and successfully migrated the two PeopleSoft ERP systems to that environment. City staff are now operating in that environment. Specific activities performed to achieve that success included:

- Development of primary and disaster recovery cloud environments in two separate data centers.
- Development and availability of adequate computing capacity for City operations.
- Migrating City systems and data to the cloud environment.
- Performance of appropriate testing of the two City systems within the cloud environment to ensure the systems functioned adequately.

Certain technical matters temporarily delayed the completion of Phase 1. The technical matters involved the City's conversion from an Oracle database (previously used) to a Microsoft Structure Query Language (SQL) database. After that matter was resolved and other activities were completed, City staff began operating in the established cloud environment effective October 10, 2016.

City Project staff's monitoring and oversight helped ensure Phase 1 was successfully implemented.

City Project staff's monitoring and oversight of those activities helped ensure the successful implementation of Phase 1. The establishment and completion of specific contractual tasks/deliverables also helped ensure Phase 1 was successfully completed. Those contractually-established tasks/deliverables (in addition to those addressed above) which were successfully completed by Ciber and/or City Project staff included:

- Completion of a comprehensive review of the City's applicable technology infrastructure to ensure a complete and accurate transfer of data from the City's internal network to the cloud environment.
- Development of detailed transition plans that outlined key steps and actions, to include system testing and target completion dates.
- Establishment of a process and timeline for incident resolution, and escalation procedures when appropriate.
- Establishment of a process to document and track City requests relative to the migration.
- Requirement to hold weekly meetings between City and Ciber Project staff during the transition process.
- Creation of secure communication paths between the City and the cloud environment (CenturyLink data centers).
- Establishment of data encryption services.
- Development of a governance plan and service guide that outlines roles and responsibilities of City and Ciber subsequent to the successful migration of City systems and data to the cloud environment.
- Installation of an Intrusion Prevention System (IPS) to protect the City's data through detection of unauthorized intrusions and

The establishment and completion of specific contractual tasks/deliverables also helped ensure Phase 1 was successfully completed.

measures to prevent those attempts from harming the network, applications, and data.

- Ongoing management and monitoring of server utilization and network bandwidth and connectivity to ensure the environment is efficiently processing data and transactions.
- Upgrade of the underlying framework used to develop and support the Financials and HR systems, PeopleTools, to a current version (version 8.54).
- Implementation of a newer server operating system from which the Financials and HR systems operate that is compatible with the upgraded PeopleTools version.
- Implementation of a newer database, SQL, which houses the data that makes up the Financials and HR systems.

At the end of our audit fieldwork, other activities were in progress to ensure efficient and secure operations subsequent to the successful transition to the cloud environment. Those activities are described below:

We recommend the City continue efforts to implement appropriate DDoS prevention measures.

- The City is responsible for establishing mitigation defenses for Distributed Denial of Service (DDoS) attacks. DDoS attacks represent instances where an individual or entity maliciously attempts to overload a website (e.g., website used in a hosted cloud environment) with more traffic (activity) than the website can handle, resulting in the website being overloaded and unavailable for use. Management is currently evaluating options to determine the appropriate mitigation measures that should be implemented to address these potential attacks. We recommend the City continue those efforts and implement appropriate DDoS prevention measures.

The City should continue efforts to establish log management practices and to ensure Ciber applies appropriate updates and patches.

- An important control to protect the City's data in a cloud hosted environment is the ongoing review of server log files by knowledgeable City staff for the purpose of detecting evidence of unauthorized activity or activity outside of established parameters. Management was in the process of establishing such log management practices for activity related to the two

PeopleSoft systems now maintained in a cloud environment. We recommend those practices be established and followed.

- As part of good practices for both hardware and software management, necessary updates and patches should be applied, and anti-virus software should be maintained and updated. In regard to the cloud environment, Ciber is contractually responsible for performing those practices on behalf of the City. Ciber asserted to City Project staff those practices are being followed.

In summary, the City has successfully transitioned the two systems to the cloud environment. Remaining actions are in the process of being taken to address management of that environment subsequent to that successful transition.

Remaining actions are being taken to address management of the cloud environment subsequent to the successful transition.

Phases 2 and 3 were started and certain activities completed. As noted subsequently in this report under "Project Challenges," the City has instructed Ciber to stop further actions in upgrading the two City PeopleSoft ERP systems and subsequent implementation of the two additional system modules and the integrated training application. Notwithstanding that circumstance, several activities relative to Phases 2 and 3 had been successfully completed as of the date those efforts were stopped. Specifically, as of the date the systems were successfully migrated to the cloud environment and operational (in use by City staff), there were 21 Project tasks/deliverables that were to be completed by Ciber and/or City Project staff in regard to upgrading the two ERP systems and implementing additional modules. We determined each of those 21 tasks/deliverables has been completed. *(Note: The City's upgrade contract with Ciber established 61 Project tasks/deliverables; the remaining 40 tasks/deliverables were due for completion subject to the successful migration. The completion of those remaining 40 tasks/deliverables will be addressed in a subsequent progress audit of the Project, conducted by our office, in the event the upgrade activities are resumed.)*

As of the date these systems were successfully migrated, there were 21 Project tasks/deliverables that were to be completed by Ciber and/or City staff in regard to subsequent Project phases; each of those 21 tasks/deliverables have been completed.

The completed 21 tasks/deliverables included the following:

- Specific City and Ciber staff were assigned to manage the Project *(one task/deliverable).*
- City staff with appropriate skills were assigned to and participated in the Project *(one task/deliverable).*
- City staff provided Ciber rules and procedures utilized by the City in the operation of the two PeopleSoft systems *(one task/deliverable).*
- Ciber created and made available to the City a website demonstrating the appearance of the upgraded system to City users *(one task/deliverable).*
- Ciber provided ten weeks of onsite functional assistance to the City *(one task/deliverable).*
- Ciber completed in-depth reviews of the City's current PeopleSoft Financials and HR systems for the purpose of documenting the City processes for completing various tasks (e.g., payroll processing, recording receivables and payables, adding newly hired employees to the system) and how the upgrade will impact those processes *(12 tasks/deliverables).*
- Ciber performed an in depth review of the two modules ("ePerformance" and "Enterprise Learning Management" modules) to determine the impact of their implementation on City workflows and operations. *(two tasks/deliverables)*
- Ciber prepared and provided City Project staff reports showing how former customizations of the City's PeopleSoft ERP systems will impact the upgrades of those systems *(one task/deliverable).*
- Ciber and City staff ensured the process to backup system data within the cloud environment continued during the upgrade process (will also be used subsequent to the upgrade completion if the Project is resumed) *(one task/deliverable).*

Project Challenges

A lack of clarity and specificity in certain contractual terms and conditions, including tasks and expected roles and responsibilities of Ciber and City staff, have caused confusion, communication issues, and delays in Project progress.

A lack of clarity and specificity in certain contractual terms and conditions, including tasks and expected roles and responsibilities of Ciber and City staff, have caused confusion, communication issues, and delays in Project progress. Based on discussions with Project management and staff and reviews of related records and correspondence, we noted areas where the City and Ciber have differed as to interpretation of certain contractual terms and conditions, to include expectations regarding roles and responsibilities of both parties. Examples of these differences follow:

- Management asserted that City Project staff assisted with the completion of certain contractual tasks that were the responsibility of Ciber. Examples of that work included (1) establishing a secure communication path (Virtual Private Network, or VPN) between the City and the cloud environment, (2) establishing employee access controls for the Financials and HR systems operating in the cloud environment, (3) transferring Financial and HR systems' data to the cloud environment, and (4) developing interfaces between various City applications (e.g., PeopleSoft CIS and Kronos, the City timekeeping system) and the cloud-based Financials and HR systems. City management interpreted these tasks as performed by City staff to be the responsibility of Ciber.

City Project staff and Ciber disagree as to the extent of annual testing that must be performed to ensure the City can effectively operate at the designated backup site in the event of a disaster.

- City Project staff and Ciber disagree as to the extent of annual testing that must be performed to ensure the City can effectively operate at the designated backup site in the event of a disaster. Specifically, while the contract provides for annual testing by Ciber of the disaster recovery site, the terms do not specify the extent of that testing. The City wants that testing to be sufficient to ensure sustained City operations for an extended period in the event of a disaster. Ciber, however, plans to provide less extensive testing that would ensure a transfer to the backup site will successfully occur, but not ensure sustained operations once that transfer (cutover) occurs.

- Ciber initially asserted to the City that the fees for the cloud host vendor (CenturyLink) would be $18,500 monthly. However, as addressed in ISSUE #6 on pages 28 to 31 of this report, that fee was significantly higher. Notwithstanding the City should have obtained a proper understanding of those fees before it executed the contracts and that Ciber has agreed to provide the City a credit due to the misunderstanding, this occurrence furthered the City's concerns as to the adequacy of Ciber's communications with the City.

As explained later in this report under "Conclusion and Project Status," these areas contributed to the City's decision to suspend the Project.

Cloud hosting services costs are exceeding initial estimates.

Cloud hosting services costs are exceeding initial estimates. As previously explained in ISSUE #6 on pages 28 to 31 of this report, the City executed a contract with CenturyLink for cloud hosting services without a complete understanding of the manner and basis on which the City would be billed for those services. As a result, the costs are significantly higher than what the City initially planned and anticipated. As previously explained, because Ciber had initially advised the City on this matter, Ciber agreed to offset this increased cost by executing a contractual change order that provided Ciber would not bill the City for hours worked on the Project by Ciber staff at the end of the Project. The value of those unbilled services is to equal $276,000, which was the estimate of the increased costs. Notwithstanding that change order, our audit shows that based on activity as of December 31, 2016, the actual increased costs will likely approximate $327,000, which is $51,000 more than the initial estimated $276,000.

City Project management indicated options are being explored to reduce subsequent hosting costs to address the unanticipated increased expenses.

City Project management indicated options are being explored to reduce subsequent hosting costs to address these unanticipated increased expenses. One such option being considered is a reduction in available system capacity during non-business hours, i.e., nights, weekends, and holidays. In addition to addressing this revised estimate during their ongoing renegotiations with Ciber, we

recommend City Project management continue with efforts to reduce hosting costs.

Conclusion and Project Status

The City's PeopleSoft Financials and HR systems were migrated to and are currently operating in a cloud environment. Accordingly, Phase 1 of the Project has been successfully completed. However, because of ongoing concerns regarding Ciber's provision of managed and upgrade services, the City directed Ciber on January 10, 2017, to suspend further Project activities in regard to the upgrade of the two PeopleSoft systems (Phase 2). In that correspondence the City informed Ciber the upgrade services were being suspended to allow the City to develop and execute amendments to the contracts that will clarify the roles and responsibilities of each party, address Project milestones, establish clearly defined deliverables, as well as penalties in the event Ciber does not meet the established milestones or provide the required deliverables (i.e., as we recommended in ISSUE #3 on pages 24 to 26 of this report).

Because of ongoing concerns regarding Ciber's provision of managed and upgrade services, the City directed Ciber on January 10, 2017, to suspend further Project activities in regard to the upgrade of the two PeopleSoft systems.

City management indicated that it is currently working on those contract amendments, which have been proposed to Ciber for execution. Management indicated that if favorable amendments cannot be executed, that it will terminate the upgrade contract in accordance with existing contractual provisions.

We recommend the City continue efforts to develop and execute contract amendments that are in the best interests of the City. As part of those efforts, we also recommend City management consider establishing a maximum price (fee) that will be paid for the remaining services. (See ISSUE #3 and our recommendation on pages 24 to 26 of this report of this report.) In determination of that maximum price, the City should properly consider the previously executed change order whereby Ciber agreed to provide the City "free" (unbilled) services valued at $276,000 to offset the higher than anticipated hosting fee. (See ISSUE #6 and our recommendation on pages 28 to 31 of this report.) In the event the City is not successful in negotiating appropriate contract

We recommend the City continue efforts to develop and execute contract amendments that are in the best interests of the City.

amendments and the upgrade contract is terminated, the City should develop alternative plans to timely upgrade the two PeopleSoft ERP systems to the current versions.

Overall Conclusion

The primary objective of this audit was to evaluate and report on the status of the City's project to transition the PeopleSoft Financials and Human Resources systems to a cloud environment and subsequently upgrade those two major systems. To date, the City has successfully completed the transition, but due to concerns with the upgrade services, has suspended the contractual work related to that endeavor. Our audit identified areas where enhancements are needed for this and future projects. Those areas pertain to competitive selection of vendors, execution of contracts that are in the City's best interest, controlling and payment of contractual expenses, and following best practices when transitioning internal systems to a cloud environment. Recommendations were provided to address the applicable areas.

We would like to thank staff in the City's Technology and Innovations Department and in Procurement Services for their cooperation and assistance during this audit.

Appointed Official's Response

City Manager Response:

We have reviewed the City Auditor's report and will take into consideration the recommendations contained in the report. Although we concur with some of the audit comments, we believe that management was diligent in reviewing and making recommendations on upgrading the city's ERP systems. During our due diligence process options and pricing for various ERP solutions including WorkDay, Fusion, and Oracle/Ciber cloud solution were evaluated. Staff from the various functional areas (accounting, budget, procurement, human resources, and equity and workforce development) spent a significant amount of time assessing the capabilities of the different systems and how they fit with the city's processes. Ultimately a decision was made by management and affirmed by the ISS Steering Committee to upgrade our existing

systems via the Oracle/Ciber cloud solution. Both the WorkDay and Fusion solutions did not provide all the necessary components for the City, were more expensive to implement than the selected option, and would require extensive retraining of the organization.

We would like to take this opportunity to provide additional comments related to the report's recommendations as well as provide a status report on actions taken to date.

Prior to release of this audit, staff had already been working on addressing issues with the Ciber contract. On January 10, 2017, the City notified Ciber of our intent to suspend all services related to the PeopleSoft 9.2 Upgrade project. Ciber was also provided a draft amendment to the Statement of Work (SOW) for their review and consideration that clarified the roles and responsibilities of each party, addressed project milestones, established clearly defined deliverables, and provided for penalties for failure to meet milestones or deliverables. After a period of discussion, the City and Ciber reached an agreement on the revised SOW on March 17th 2007. The revised agreement is currently being processed and it is anticipated that work on the PeopleSoft upgrade will resume in April of 2017.

As it relates to issues related to conflict of interest, management has already approved a change to the city's procurement procedures that require city staff selected to serve on procurement evaluation teams to affirm, in writing, that no conflict of interest exists. These changes were also presented to the Independent Ethics Board for their review and staff is currently in the process of updating the City's procurement procedures to reflect this new requirement. We will further enhance these requirements by establishing a time frame whereby staff with prior employment history with a vendor under consideration would not be able to participate in procurement related decisions for a period of two years.

The City has historically utilized state contracts, General Services Administration (GSA) contracts, and piggy backing onto other governmental contracts to procure goods and services and as these contracts have already gone through a competitive process. This

process has served the City well over the years and management will continue to assess the use of these while taking into consideration the recommendations contained in this audit.

We appreciate the City Auditor and his staff's work on this audit and the cooperation of city staff during this review.

This page intentionally left blank.

Appendix A: Additional Best Practices

Best Practice	Practice Followed?
1. Organizations using cloud hosted services should be aware of the information retained by the cloud host (vendor) regarding the organization's specific IT network and activities, such as data volumes or locations of users that access the cloud-based services. Additionally, organizations should be made aware of the circumstances in which that information is made available to third parties by the cloud host.	Yes
2. Organizations should analyze the cloud service provider's formal information security policies to ensure up-to-date security technology and processes are being used, and to also ensure security procedures for the cloud environment meet or exceed the organization's standards.	Yes
3. Organizations should have a process or contractual provisions to block third party vendor access to the cloud hosted systems and data when that access is no longer needed.	Yes
4. Prior to transitioning to a cloud environment, organizations should ensure there is sufficient bandwidth to successfully operate in that environment.	Yes
5. Organizations should ensure the cloud service provider has a reasonable process for handling DDoS attacks and data breaches, and require the provider to notify the organization in the event of any unauthorized breach within the data center housing the organization's data.	Yes
6. The organization's contract with the cloud service provider should include language stating the provider will "defend and hold harmless" the organization in the event of unauthorized access to the organization's data, such as a breach.	Yes
7. The organization's contract with the cloud service provider should include the organization's right to audit the provider's processes, controls, and actions relevant to the organization.	Yes
8. The cloud service provider should be required to notify the organization in the event the provider no longer maintains relevant industry certifications.	Yes
9. The organization should establish a change management strategy to govern the cloud migration process and system upgrades within the cloud environment.	Yes
10. Organization employees should be trained on system changes necessitated by the migration to the cloud environment.	Yes
11. The organization should determine how the cloud service provider controls physical access to its data center, including the server room.	Yes

12. The organization should ensure the cloud service provider requires visitors to sign in and be escorted at all times they are inside the provider's data center.	Yes
13. The organization should ensure the cloud service provider requires data center employees to display identification badges while at work.	Yes
14. The organization should verify secure areas of the cloud service provider's data center are monitored by closed circuit television.	Yes
15. The organization should verify the cloud service provider performs adequate background checks on employees granted access to the provider's data center.	Yes
16. The organization should verify its data is segregated within the data center from the data of other users (customers).	Yes
17. To ensure proper management and oversight, the organization should verify the cloud services provider has administrator access to the entire data center.	Yes
18. The organization should ensure the cloud service provider has an adequate plan to protect the organization's data in the event of a man-made or natural disaster.	Yes
19. The organization should have the right to allow, deny, or delay system upgrades or changes to the data center's servers housing the organization's data.	Yes
20. The organization should evaluate the cloud service provider's planned downtime procedures for their impact on the organization's operations.	Yes
21. Organizations should require the use of geo-blocking measures to preclude remote computers located outside of a defined geographical area from accessing the cloud-based systems and data.	No *(Note)*
Note: This circumstance is addressed on page 46 of this report.	

Appendix B: Management Action Plan

Action Steps	Responsible Employee	Target Date
Administrative and Professional Services		
1) The Procurement Policy (Commission Policy 242) will be revised to specify a period of time that must have passed since an employee's employment with a potential vendor before that employee will be allowed to participate in evaluations and/or selections of proposals for City business from that previous employer.	Patrick Twyman	September 30, 2017
2) The City will revise the City Procurement Policy to require employees involved in evaluating and/or selecting potential City vendors to complete a signed assertion indicating they are independent of and have no conflicts of interests with the vendors being evaluated.	Patrick Twyman	September 30, 2017
Technology and Innovation		
3) For future IT projects of the nature addressed in the audit, efforts will be made to ensure competitive procurement practices are followed in accordance with the intent of City policy and provisions of piggybacked contracts.	Tim Davis	January 1, 2018
4) For future City IT endeavors that are project-like in nature, and are a significant expenditure, applicable contracts will be executed for a firm amount, or an amount not to exceed a firm amount as appropriate, and when to the advantage of the City, so as to reduce the City's exposure to financial risk.	Tim Davis	January1, 2018
5) For future IT projects of the nature addressed in the audit, applicable contracts will be executed that establish project milestones, and penalties that can be applied in the event the contractor does not meet those milestones.	Tim Davis	January 1, 2018
6) For future City IT projects of the nature addressed in the audit and which involve a defined set of tasks and a completed end product, performance bonds will be required and obtained from applicable contractors.	Tim Davis	January 1, 2018
7) For future City IT projects of the nature addressed in the audit, applicable contracts will require or provide for (1) adequate and appropriate levels of insurance coverages, (2) the City to be listed as an additional insured on applicable contractor insurance coverages, and (3) that the City will be held harmless for actions attributable to the contractor.	Tim Davis	January 1, 2018

Action Steps	Responsible Employee	Target Date
8) For future City IT projects of the nature addressed in the audit, project management will consult with the Risk Management Division, prior to execution of the contracts, to determine the levels of insurance that are appropriate to require of proposed contractors.	Tim Davis	January1, 2018
9) For future City IT projects of the nature addressed in the audit, project management will obtain a proper and complete understanding of billing provisions of potential vendors, prior to executing contracts with those vendors.	Turquoise James	January 1, 2018
10) For future City IT projects of the nature addressed in the audit, project management will review invoices in a manner to ensure the City is billed in accordance with applicable contractual terms and conditions.	Tim Davis	January 1, 2018
11) For future City IT projects of the nature addressed in the audit, vendor/contractor invoices will be (1) stamped as to date of receipt and (2) timely reviewed and paid by appropriate staff.	Turquoise James	September 1, 2017
12) For future City IT projects of the nature addressed in the audit, designated project managers will document their review and approvals of vendor and contractor invoices.	Tim Davis	July 30, 2018
13) For future City IT projects of the nature addressed in the audit, applicable support provided with vendor invoices will be retained in City files (record systems) in accordance with City record retention schedules.	Turquoise James	September 1, 2017
14) For future City IT projects of the nature addressed in the audit, efforts will be made to better plan and schedule onsite work by contracted employees such that contractors do not incur re-scheduling costs that are reimbursed by the City.	Tim Davis	January 1, 2018
15) For future City IT projects of the nature addressed in the audit, terms will be negotiated with contractors/vendors that establish reasonable and maximum amounts that will be reimbursed for contractor/vendor travel and lodging costs. Provisions in the City travel policy will serve as a guideline for that purpose.	Tim Davis	July 30, 2018
16) For future migrations of City systems to a cloud environment, appropriate load testing will be performed to ensure the applicable environment can efficiently and effectively process the expected volume of transactions and activity.	Tim Lee	September 1, 2018

Action Steps	Responsible Employee	Target Date
17) For the Project addressed in this audit, consideration will be given to developing a formal plan to guide City staff in the event the City leaves the current cloud provider.	Tim Davis	July 30, 2018
18) For the Project addressed in this audit, the ongoing evaluation to determine the impact of additional encryption of City data maintained in the cloud environment will be completed. Appropriate actions will be taken based on the evaluation results.	Tim Lee	September 30, 2017
19) System access will be obtained from Ciber that will allow designated City staff to determine the individuals granted access to City data and IT resources by Ciber. Identified individuals will be required to assert they agree to abide by appropriate City policies and procedures pertaining to City IT resources and data. Consideration will be given for geo-blocking of existing Ciber managed cloud environment	Tim Davis	September 1, 2017
20) A comprehensive City policy on cloud computing will be established and adopted that will include: • Review appropriate independent IT audit reports to determine if the applicable cloud environment (includes data centers) is reasonably secure and protected. Those reports will be obtained and used during the vendor selection process and reviewed as appropriate. • Consideration will be given to implementing geo-blocking measures for the current and future cloud environment • Appropriate log management practices will be implemented	Tim Davis and Tim Lee	March 31, 2018
21) Appropriate DDoS prevention measures will be implemented for the two PeopleSoft systems transitioned to the cloud environment.	Tim Lee	August 30, 2018
22) Appropriate plans will be implemented to validate Ciber is applying necessary updates and patches to the hardware and software being used in the City's cloud environment. Appropriate log review will occur to insure data integrity.	Tim Lee	September 1, 2017
23) Efforts to identify and implement ways to reduce cloud hosting and management costs associated with the two migrated PeopleSoft systems will continue.	Tim Davis	January 1, 2018

24) Efforts will continue to develop and execute contract amendments with Ciber that are in the best interest of the City; specifically, to clarify the roles and responsibilities of both parties, establish milestones for the remaining portion of the Project, establish more clearly defined deliverables, and establish financial incentives for Ciber to meet the milestones and provide the deliverables. Additionally, consideration will be given to establishing a maximum fee that will be paid to Ciber for the remaining upgrade services. The previously executed amendment whereby Ciber agreed to provide free services valued at $276,000 at the end of the upgrade will be considered in the negotiation process for these contract amendments.	Tim Davis	April 28, 2017