Sonoma County

Auditor-Controller-Treasurer-Tax Collector

Internal Audit Report

County of Sonoma
PeopleSoft Enterprise Financial System
Post Implementation Review

Engagement No: 4045
Report Date: January 24, 2018

Erick Roeser
Auditor-Controller-Treasurer-Tax Collector

ERICK ROESER
AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR
585 FISCAL DRIVE, SUITE 100
SANTA ROSA, CA 95403
PHONE (707) 565-2631
FAX (707) 565-3489

JONATHAN KADLEC
ASSISTANT AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

AMANDA THOMPSON
ASSISTANT AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

Kanchan K. Charan, CPA	Audit Manager
Damian Gonshorowski, CPA	Audit Supervisor
Ryan Burns, CISA	Auditor-In-Charge

Auditor-Controller-Treasurer-Tax Collector Web Site
http://sonomacounty.ca.gov/Auditor-Controller-Treasurer-Tax-Collector/

Table of Contents

PeopleSoft Enterprise Financial System
Post Implementation Review
Engagement No. 4045
Report Date: January 24, 2018

Executive Summary

As a part of the 2016/2017 Annual Audit Plan, the Internal Audit Division (Internal Audit) of the Sonoma County Auditor-Controller-Treasurer-Tax Collector's (ACTTC) Office conducted a Post Implementation Review (PIR) over the County of Sonoma's PeopleSoft Financials core application of the Enterprise Financial System (EFS).

The following were the objectives of the PIR:

1. Evaluate the County's controls in place over key areas of the implementation of EFS, and;
2. Where opportunities for improvement are identified, make appropriate recommendations to management to assist current functionality and or future critical organizational Information Technology (IT) projects

There is one finding and two observations relating to overall system availability.

Finding:

Finding 1 – The ACTTC Office should, in conjunction with the Information Systems Department (ISD), develop a business continuity and disaster recovery plan covering all systems it uses.

Management Response to Finding 1:

ACTTC Management is in agreement that a comprehensive Disaster Recovery/Business Continuity (DR/BC) plan covering all IT systems administered by ACTTC personnel should be developed, put into play and tested annually.

Observations:

Observation 1: The EFS Team should continue to develop procedures for increasing the frequency of user access review from once a year to quarterly.

Management Response to Observation 1:

The EFS Support Organization concurs with Observation 1, and has implemented a quarterly end user access review process.

Observation 2 – The EFS Team should continue to review, evaluate and implement the recommendations contained in the Security Assessment report issued by ISD

The implementation of EFS utilized methods and protocols supported by best practices resulting in a functional system that adequately meets the requirements of the County. We would recommend that implementation of other major systems in the County be patterned after the EFS project.

Management Response to Observation 2:

The EFS Support Organization concurs with Observation 2. Several of the recommendations made as a result of the ISD security assessment have already been implemented, with others where there is agreement with the recommendations having been incorporated into the EFS Work List of desired system functionality and improvements.

Introduction and Background

Introduction

The Internal Audit Division of the ACTTC completed the County's PeopleSoft Enterprise Financial System (EFS) Post Implementation Review (PIR). We conducted the PIR in accordance with the *International Standards for the Professional Practice of Internal Auditing (Standards).* These Standards require that sufficient information and evidence to achieve audit objectives are identified, evaluated and documented. The evidence obtained provides a reasonable basis for the results, observations, and recommendation contained in our report.

The purpose of this audit report is to furnish management independent and objective analyses, recommendations and other information concerning the activities reviewed. The audit report is a tool to help management identify and implement improvements.

The Internal Audit Division as well as the Assistant Auditor-Controller-Treasurer-Tax Collector, who is responsible for the implementation of EFS, report to the elected Auditor-Controller-Treasurer-Tax Collector. Except for conducting this review, the Internal Audit Division has no other responsibilities or involvement in the management or performance of functions relating to the EFS implementation.

Background

The Oracle/PeopleSoft EFS project was a significant application implementation impacting County departments and all users of the County's financial systems including special districts and other governmental entities. Post Implementation Reviews (PIR) are used to evaluate the effectiveness of the system development after the system has been in production for a period of time (6 months to 2 years after "go-live"). A basic PIR reviews certain areas at a high level to ensure:

- Business requirements have been met
- Expected benefits have been realized
- The system is considered usable
- Internal and external stakeholders' expectations are met
- Key risks are mitigated
- Change management installation and accreditation processes were performed effectively and efficiently

The County's Financial Accounting Management Information System (FAMIS) was a mainframe system used by all departments and agencies of the County to manage financial and accounting transactions and produce reports across all lines of County business. FAMIS was installed over 30 years ago and had reached its end of life and was no longer actively supported by the system vendor.

The County considered acquiring an integrated and automated set of systems to serve as a core enterprise-wide financial management system. Through a request for proposal (RFP) process facilitated by the Government Finance Officers Association (GFOA), the County decided on the Oracle/PeopleSoft Enterprise Financial System. The proposed EFS was approved by the Board of Supervisors in September 2012. PeopleSoft was chosen as the software vendor with Ciber being the technical implementer.

The implementation spanned a period of 33 months starting September 2012. The implementation team included staff and management from various County Departments structured into Project (staff) and Leadership (management) Teams as well as a Steering Committee consisting of the County Administrator, ACTTC and Director of Information Systems. The Director of General Services and the Director of Human Resources joined the Steering Committee post implementation. The implementation was accomplished in two phases as detailed below:

Phase 1 achieved go-live status on July 1, 2014, with the following modules implemented:

1. General Ledger
2. Accounts Payable
3. Purchasing and eProcurement
4. E-supplier (implemented February 2015)
5. Asset Management

Phase 2 achieved go-live status July 1, 2015, with the following modules implemented:

1. Accounts Receivable
2. Project Costing
3. Grants Management
4. Contracts
5. Strategic Sourcing (implemented February 2015)
6. Hyperion Budget

Objectives, Scope & Methodology

Objectives

In 2014, ACTTC's Internal Audit Division conducted a county wide risk assessment that identified ACTTC's General Accounting function as having inherently high potential risk, primarily due to the volume of transactions processed in its financial system and the need for reliable information to produce mandated financial reports and disclosures. In discussion with the ACTTC and the Audit Committee, it was determined that a PIR of the newly implemented system should be performed prior to the planned audit of the General Accounting function. The following were the objectives of the PIR:

1. Evaluate the County's controls in place over key areas of the implementation of EFS, and;
2. Where opportunities for improvement are identified, make appropriate recommendations to management to assist current functionality and/or future critical IT projects.

Scope

The County's Enterprise Financial System (EFS) is comprised of PeopleSoft Financials and Hyperion Budgeting as well as multiple supporting applications. The focus of the PIR review conducted focused on the core PeopleSoft Financials application only.

Based on Management's feedback and the inherent risks identified with PIR projects, Internal Audit focused on the following key areas:

1) **Project Governance** – The process that provides oversight ensuring that a system is purchased and implemented in alignment with the County's business purpose, providing the intended value. We reviewed the following key components of this process:

   a. **Program & Infrastructure Acquisition and Development** – Ensures that project approvals were obtained and appropriate project oversight was established;
   b. **Development Methodology** – Ensures a framework is used to structure, plan, and control the process of developing and implementation an Information Systems application;
   c. **Control Identification and Testing** – Ensures that appropriate controls were identified and implemented throughout the project.

2) **User satisfaction, training and system changes / enhancements** – This process provides assurance that users are involved as necessary to ensure their needs are met and are sufficiently trained to optimally benefit from system features. We reviewed the following key components of this process:

   a. **User Training and Feedback** – Ensures that appropriate level of user training is provided and user feedback is incorporated into the development of the system;
   b. **System and User Control Documentation** – Ensures that controls over the system and users (access) were identified and implemented;
   c. **Testing and Test Work Review and Approval** – Ensures that the end user testing was conducted, reviewed and approved prior to the system going live;
   d. **Tracking and Resolution of User Issues** (ISD and EFS Team Support) – Ensure system and user issues are tracked, reviewed, and resolved timely.

3) **Data Quality** – This process provides assurance that data was accurately converted and transferred from the old system to the new system. We reviewed the following key components of this processes:

a. **Testing and Test Work Review and Approval** – Ensures that adequate test work of the new system was performed and the test work was reviewed and approved to move to the next stage of implementation;
b. **Data Migration** – Ensures that data migrated from the old system is complete and accurate.

4) **System Security** – This process provides assurance that the system and data are adequately protected. We reviewed the following key components of the process (Limited scope as ISD conducted intensive Application Security Assessment for EFS):

a. **User Access –** Ensures that user access is set at acceptable levels and there is adequate segregation of access rights;
b. **System Audit Trails –** Ensures that all user activities are adequately documented by the system;
c. **Disaster Recovery –** Ensures there is adequate preparation for disasters by developing a disaster recovery plan that is periodically tested.

Methodology

To address the review objectives, Internal Audit conducted the following activities:

- Distributed a questionnaire to gather relevant information;
- Conducted general interviews and observations with key personnel;
- Reviewed extensive documentation key to the review objectives;
- Reviewed relevant standards and guidance for system implementation practices to identify key controls and activities that should be in place for large scale IT projects.

Results

Internal Audit reviewed the following areas: Governance, User Satisfaction & Training, Change Management, Data Quality, and System/Application Security.

Governance

Governance, in the context of an IT implementation, refers to the oversight needed to ensure the project has been approved, stakeholder involvement is adequate, the project stays on schedule and on task, and the budgetary goals are achieved.

We evaluated the EFS project Governance and noted the following:

- The County initiated a number of best practices with the implementation of the EFS:
    - Established an executive Steering Committee led by the County Administrator and included the ACTTC, and Director of Information Services the Director of General Services and Director of Human Resources joined the Steering Committee post implementation.
    - Partnered with GFOA in defining and gathering requirements and facilitation of a RFP.
    - Hired consultant to oversee implementation.
    - Dedicated experienced staff from various County Departments.
    - Established a separate office space for the implementation team.

- The County Board of Supervisors approved the EFS project budget which was supported by properly described deliverables and timelines to achieve them and governance structure to ensure success. The EFS Team provided updates to the County Board on a quarterly basis throughout the implementation process.

- There was sufficient documentation to support that during the project there were properly functioning steering committee, leadership team and project team. Each had clearly defined responsibilities and reporting lines for accountability.

User Satisfaction & Training

The County established extensive user training programs throughout the implementation process for phase 1 and phase 2. Initial training was available in live settings with subsequent and additional training offered online. The implementation consultants worked with the EFS project team to develop the initial training program.

- Throughout the process, the County sought end user input to ensure proper functionality of the various modules of the application.

- On a periodic basis, the County sends out user satisfaction surveys to gauge end user experiences with the system and to determine if there are any areas of improvement that need to be reviewed. Data from the surveys is evaluated, compiled and shared with appropriate management.

- Surveys conducted support that users have become increasingly more satisfied with the system and the training they receive since implementation.

Results

Change Management - System Changes / Enhancements

The EFS Team established a Change Management program for all changes to the production environment. The EFS Team utilizes the ISD Service Manager ticketing system for recording and tracking Service and Incident requests as well as logging System Change Requests. System Change requests are also recorded in an accumulated Excel worksheet (the Consolidated Work List) and are reviewed and vetted to see if changes should and can be implemented and moved to the production environment.

Based on our review, the EFS Team properly documented all change requests and ensured appropriate testing prior to migrating the changes to the production environment.

Data Quality

Data Quality refers to the basic data accuracy and reliability for a new implementation to ensure data was migrated into the new system accurately and completely through testing and other procedures. The EFS Team performed and documented the following:

- A considerable effort was made working with various departments to document and map their existing processes to incorporate into the design of the system. Detailed flowcharts were created and utilized.

- The EFS Leadership Team and Steering Committee made the decision not to migrate existing transactional detail from the FAMIS to EFS. Account Balances were converted to the new system. Testing was done to ensure the accounts were transferred completely and accurately. Examples of the test work include:

  - EFS beginning General Ledger balances were confirmed against FAMIS closing balances.

  - 1099 data extracted from FAMIS was validated against EFS withholding tables.

  - Encumbrances were validated by comparing the purchase orders in FAMIS to the Purchase Order tables in EFS.

  - Capital Assets were compared to their source data.

  - Accumulated Depreciation for Capital Assets was compared to source data.

  - During Phase II, converted beginning Accounts Receivable information from Sonoma County Water Agency (SCWA) was validated by SCWA.

  Based on our review of documentations maintained, the EFS Team followed adequate procedures to ensure data was accurately transferred from the old system to the new.

System/Application Security

An essential part of any system implementation concerns security of the system and stored data to ensure system availability, integrity, and confidentiality. As part of our review, we noted ISD conducted an overall Security Assessment of the system and included specific recommendations to strengthen the overall security of the system. Management is currently reviewing and working on the recommendations (contact EFS Project Team or

ISD Management for further information). Given the security assessment conducted by ISD, Internal Audit focused on two specific areas: end-user access and system availability.

User Access

In order to keep the system and its functions and data secure, it is important to establish policies and procedures that allow user access based on business need. Access provided over and above the business need results in increased risk with no potential benefit.

In order to methodically provide access based on need, the EFS Team developed user access profiles that are most likely to meet the needs of the user departments. In doing so, the team ensures each user profile developed does not access functions considered incompatible.

Departments fill out an EFS access form and select the user's profile from a selection of access options developed by the EFS Team that best meet their business needs. If a custom profile is requested, the EFS Team will review to ensure the user does not have access to incompatible functions before approving.

Our review supports that user access profiles were developed to ensure users do not have access to incompatible functions. All custom user requests are reviewed for access to incompatible functions before approval. The team maintains adequate documentation supporting appropriate department approvals and EFS Team reviews and approves. On an annual basis, the EFS Team work with County Departments and conducts a User Access Review to ensure access and access levels are still appropriate. Procedures are currently being developed to do such confirmation on a quarterly basis.

System Availability

In order to ensure the system is available, a number of maintenance activities need to be performed timely and effectively. Some of those activities include server and hardware maintenance, network maintenance, implementation of software patches and upgrades, and implementation and testing of Business Continuity and Disaster Recovery plans. The EFS Team works with ISD to review and perform standard as well as emergency maintenance and changes to the production environment. If target availability rate is not met, investigations will identify improvements that would be needed.

The EFS Leadership Team decided the target system availability would be 6:00 a.m. to 10:00 p.m. Monday through Sunday, with support available during normal business hours of 7:00 a.m. to 6:00 p.m. The team investigates unanticipated down times and takes actions as appropriate, reducing the risk of the systems being down for extended period of time.

2017 System Availability:

Month	System availability
January	99.56%
February	99.24%
March	100%
April	100%
May	99.53%
June	99.82
July	100%
August	99.82

Results

The percentages reflected above encompass all of EFS including Hyperion Budgeting and EFS Reporting Services. PeopleSoft availability as a stand-alone item would be an even higher percentage.

The EFS Team works in conjunction with ISD to schedule and perform routine maintenance on the EFS systems and servers to ensure servers and hardware are updated and performing efficiently and the network is stable. The EFS Team and ISD also review software patches and upgrades, to ensure they are tested and approved prior to moving to the production environment with minimal interruption to EFS users.

As noted in Change Management (page 7 of this report), the EFS Team utilizes the ISD Service Manager ticketing system for recording and tracking Service and Incident requests. The EFS Team sends out a network wide communication if there are any major issues with the system that cause an outage.

EFS has been installed on equipment at the Emergency Operations Center (EOC) on the County campus; this instance is refreshed daily from the previous night's production backup. The team is currently working on a plan to test the process. Currently, the application installed at the EOC is limited in functionality (e.g., no internet-facing web servers for Purchasing, no ability to print vendor checks). ISD will continue to meet with the EFS Team to assess ACTTC's ability to conduct critical business during a disaster.

Findings, Recommendations and Management Responses

Finding 1: **ACTTC should develop Business Continuity and Disaster Recovery plans.**

Risk Classification: B – Significant Control Weakness

Activities to ensure appropriate disaster recovery test work and Business Continuity Plans are not in place. However, ISD makes backup tapes of the EFS data nightly. On a periodic basis, the EFS Team utilizes a backup tape to update the data in the Development EFS system.

All business systems critical to an organization's continued operation must be a part of a comprehensive business continuity plan to minimize impact on its goals and objectives in the event of a disaster. ACTTC functions are critical to the operation of the County and if not available for extended periods, will negatively impact countywide operations.

Recommendation

ACTTC Management should work with ISD to develop a Comprehensive Business Continuity and Disaster Recovery Plan (BC Plan) covering all IT systems administered by ACTTC personnel. Recovery target should be established based on a comprehensive risk assessment that takes into account stakeholder needs. The Business Continuity Plan should include:

- A list of all IT systems administered by ACTTC should be established and prioritized to ensure the most critical systems are made functional first after a disaster.
- The amount of time it will take to bring each system online should be estimated and the impact on business continuity should be assessed.
- The lengths of time the operating units will be able to work off line should be estimated and the issues that will arise as a result. The plan should address these issues and provide for appropriate level of resources.
- Each system listed should be tested annually to ensure recovery is possible and efficient (Disaster Recovery Testing).

Management Response to Finding 1:

ACTTC Management is in agreement that a comprehensive Disaster Recovery/Business Continuity (DR/BC) plan covering all IT systems administered by ACTTC personnel should be developed, put into play and tested annually.

Currently, DR/BC varies from system to system as to levels of existence, planning, sophistication and maturity. Moving forward ACTTC management will work towards the development and administration of a coordinated, comprehensive and prioritized DR/BC plan encompassing all ACTTC IT systems that addresses system recovery time and data recovery point objectives.

Specific to EFS, DR/BC has previously been identified as a top priority item and significant strides have been achieved, while acknowledging that significant efforts remain to have a complete and practical DR/BC plan in place.

EFS Accomplishments to date in regards to DR/BC include:

- Collaborative discussions with ISD to identify critical business needs and the desire restoration timeframe of those needs.
- Established processes to capture nightly backups of EFS production Data.
- Installation of redundant PS application and hardware at the County Emergency Operation Center (EOC).
- Identification of 3 disaster scenarios to be addressed:
    - ISD Data Center lost or degraded, other county buildings lost.
    - ISD Data Center functioning but staff cannot approach.
    - Loss of Data Center and other county buildings.
- As a direct result of the recent wildfires, established a presence on the Microsoft Azure cloud.
- Establishment of working group, consisting of ACTTC and Information Systems Department (ISD) staff, to develop and expand EFS DR/BC.

Continuing/additional efforts include:

- Test the process of restoring backups within the Azure cloud as an offsite disaster recovery environment.
- Re-review of critical functions and applications to determine:
    - Recovery Time Objective – how soon application(s) to be restored.
    - Recovery Point Objective – how old can the data be when it is restored.
- Review of server requirements for the application.
- Development of cost forecasts for the identified disaster scenarios
- Development and deployment of DR/BC plan to address all disaster scenarios that are effective, efficient and economically feasible.
- Performance of annual testing of developed DR/BC plan(s).

DR/BC is an acknowledged critical need of the ACTTC, and focused attention will be provided to EFS, as well as all other ACTTC administered IT systems, moving forward.

Observation 1 – EFS Team should continue to develop and implement procedures for performing user access reviews more frequently.

Periodically, user access reviews should be performed to reduce the risk that users continue to have access to the system without a business purpose. Although controls are in place to ensure access is provided only to employees with a business purpose, there is a risk that employees whose business purpose has expired continue to have access. The EFS Team currently performs this review annually and plans to perform the review on a quarterly basis in the future. We encourage the team to continue to develop procedures to move from an annual to quarterly review to further reduce the risk of unauthorized use of the system.

Management Response to Observation 1:

The EFS Support Organization concurs with Observation 1, and has implemented a quarterly end user access review process. On a quarterly basis all PeopleSoft users IDs will be queried to identify the last respective login date to EFS. Once identification has been made of users that have not accessed the system for a period of 6 months, user departments will be contacted to request the EFS access Request form needed to deactivate a User ID. Additionally, as part of the department contact effort there will be a reminder for department to review current employee permissions.

The quarterly PeopleSoft User Account Review procedure was implemented in December 2017. Intent is that following a period of 2 quarters to allow for refinement of the procedure, the process will be expanded to include additional EFS applications.

Observation 2 - EFS Team should continue to review, evaluate and implement the recommendations contained in the Security Assessment report issued by ISD

In June 2017, the EFS Leadership Team responded to the recommendations outlined in the EFS Security Assessment conducted by ISD. To date, the EFS Team has implemented or is in the process of implementing eight out of the 17 recommendations and is in the process of evaluating or has determined the cost outweighs the benefits on the remaining nine.

Management Response to Observation 2:

The EFS Support Organization concurs with Observation 2. Several of the recommendations made as a result of the ISD security assessment have already been implemented, with others where there is agreement with the recommendations having been incorporated into the EFS Work List of desired system functionality and improvements. Items having been placed on the Work List are prioritized along with all other desired system improvements and are dependent upon Support Organization resource capacity for resolution.

EFS Support Organization has requested additional cost information from ISD for 2 of the recommendations made. Requested cost information will allow for the thorough cost benefit analysis for determination if the items are to be added to the Work List, or if the involved cost outweighs any potential benefit and the recommendations will not be incorporated into EFS.

It was agreed upon by the EFS Leadership Team to request an annual security assessment from ISD, from the perspective of progress on previous recommendations, as well as any new compliance or industry standard matters and best business practices.

Conclusions and Staff Acknowledgement

Conclusions

Implementing a new integrated Enterprise Financial System is a significant undertaking that affects every department in the County as well as mandated and non-mandated financial reporting requirements.

The County took the necessary steps such as selecting a vendor with experience implementing an EFS in a Public Service environment, hiring a project manager with experience in Oracle system implementations, and setting up a project team and leadership structure to ensure the project was completed within the defined expectations.

The EFS Team should continue to work on developing the User Access Reviews and Business Continuity/Disaster Recovery Testing.

The implementation of EFS utilized methods and protocols supported by best practices resulting in a functional system that adequately meets the requirements of the County. We would recommend that implementation of other major systems in the County be patterned after the EFS project.

Staff Acknowledgement

We would like to thank ACTTC Management and the EFS Team for their time, information, and cooperation throughout the review.

Appendix A: Report Item Risk Classification

For purposes of reporting audit and/or review findings and recommendations, report items are classified into three distinct categories to identify the perceived risk exposure:

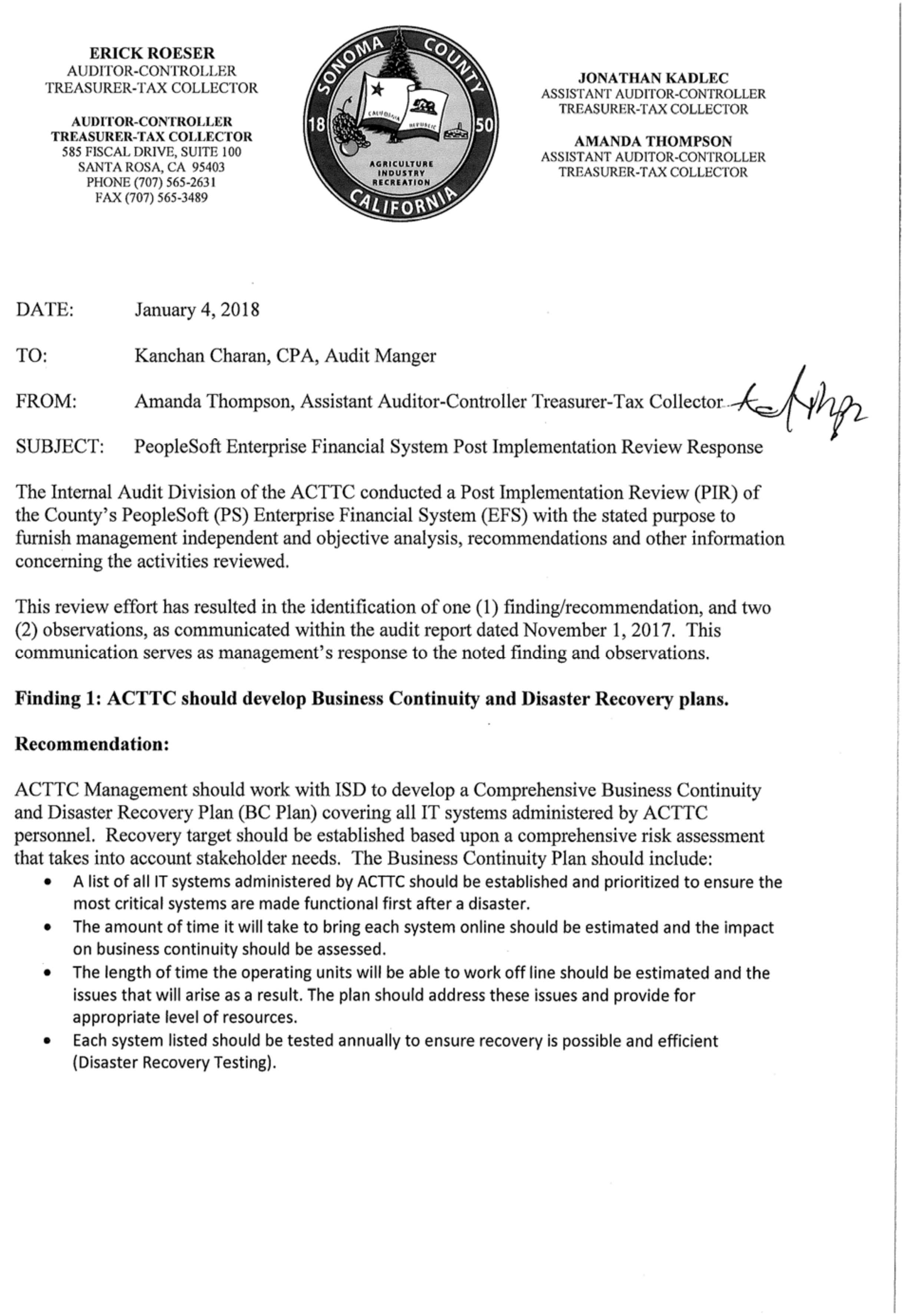
- **Risk Classification A: Critical Control Weakness:**
  Serious audit findings or a combination of Significant Control Weaknesses that represent critical exceptions to the audit objective(s), policies, and/or business goals of a department/agency or the County as a whole. Management is expected to address Critical Control Weaknesses brought to their attention immediately.

- **Risk Classification B: Significant Control Weakness:**
  Audit findings or a combination of Control Findings that represent a significant deficiency in the design or operation of internal controls. Significant Control Weaknesses generally will require prompt corrective actions.

- **Risk Classification C: Control Findings:**
  Audit findings concerning internal controls, compliance issues, or efficiency/effectiveness issues that require management's corrective action to implement or enhance processes and internal controls. Control Findings are expected to be addressed within our follow-up process.

The current status of implementation of recommendations will be followed up no later than the end of the second fiscal year after the report has been issued. Critical control weakness findings will be followed up between six months and one year of the date of the report.

Appendix B: Management Responses



ERICK ROESER
AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR
585 FISCAL DRIVE, SUITE 100
SANTA ROSA, CA 95403
PHONE (707) 565-2631
FAX (707) 565-3489

JONATHAN KADLEC
ASSISTANT AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

AMANDA THOMPSON
ASSISTANT AUDITOR-CONTROLLER
TREASURER-TAX COLLECTOR

DATE: January 4, 2018

TO: Kanchan Charan, CPA, Audit Manger

FROM: Amanda Thompson, Assistant Auditor-Controller Treasurer-Tax Collector

SUBJECT: PeopleSoft Enterprise Financial System Post Implementation Review Response

The Internal Audit Division of the ACTTC conducted a Post Implementation Review (PIR) of the County's PeopleSoft (PS) Enterprise Financial System (EFS) with the stated purpose to furnish management independent and objective analysis, recommendations and other information concerning the activities reviewed.

This review effort has resulted in the identification of one (1) finding/recommendation, and two (2) observations, as communicated within the audit report dated November 1, 2017. This communication serves as management's response to the noted finding and observations.

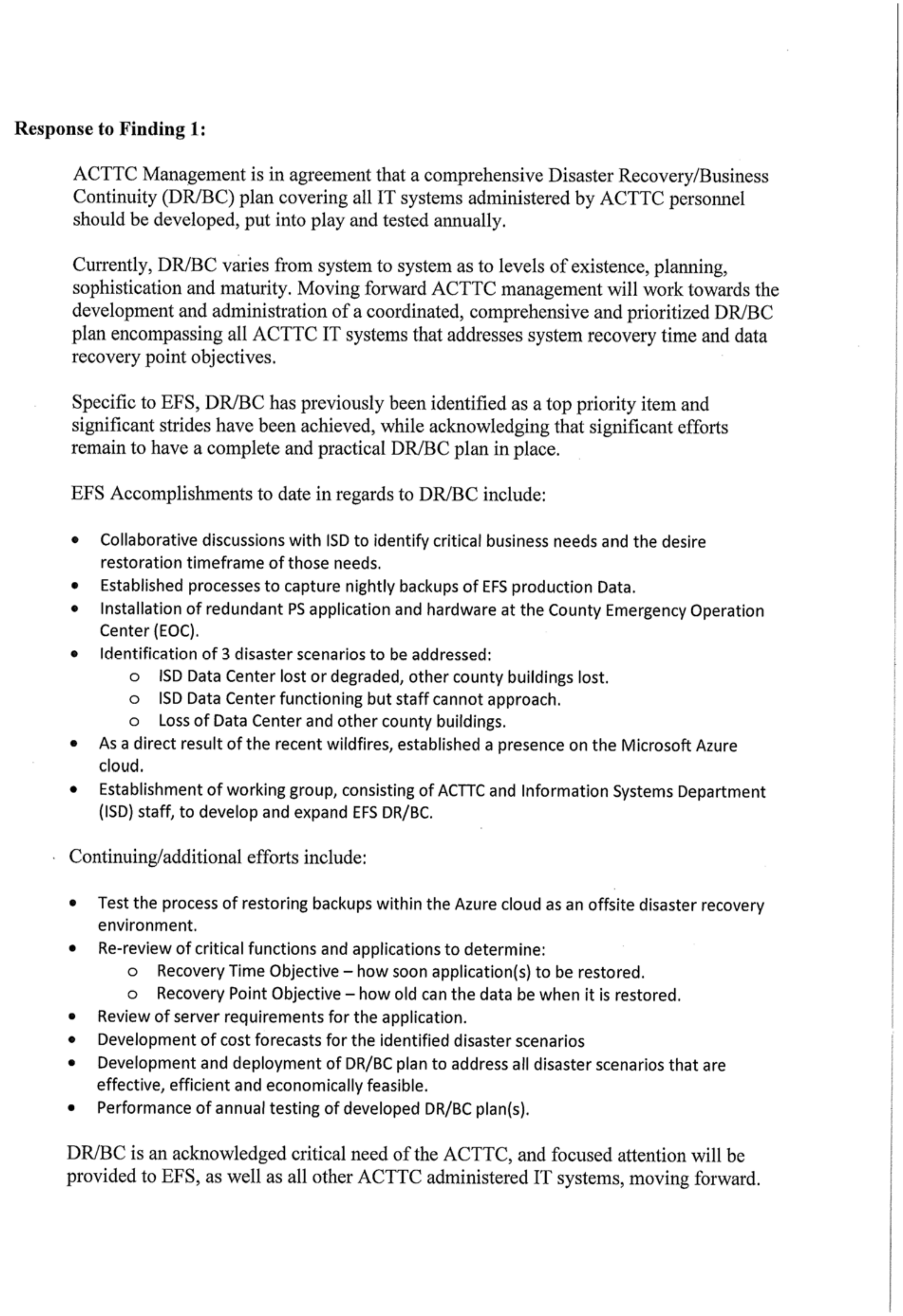
Finding 1: ACTTC should develop Business Continuity and Disaster Recovery plans.

Recommendation:

ACTTC Management should work with ISD to develop a Comprehensive Business Continuity and Disaster Recovery Plan (BC Plan) covering all IT systems administered by ACTTC personnel. Recovery target should be established based upon a comprehensive risk assessment that takes into account stakeholder needs. The Business Continuity Plan should include:

- A list of all IT systems administered by ACTTC should be established and prioritized to ensure the most critical systems are made functional first after a disaster.
- The amount of time it will take to bring each system online should be estimated and the impact on business continuity should be assessed.
- The length of time the operating units will be able to work off line should be estimated and the issues that will arise as a result. The plan should address these issues and provide for appropriate level of resources.
- Each system listed should be tested annually to ensure recovery is possible and efficient (Disaster Recovery Testing).

Appendix B: Management Responses



Response to Finding 1:

ACTTC Management is in agreement that a comprehensive Disaster Recovery/Business Continuity (DR/BC) plan covering all IT systems administered by ACTTC personnel should be developed, put into play and tested annually.

Currently, DR/BC varies from system to system as to levels of existence, planning, sophistication and maturity. Moving forward ACTTC management will work towards the development and administration of a coordinated, comprehensive and prioritized DR/BC plan encompassing all ACTTC IT systems that addresses system recovery time and data recovery point objectives.

Specific to EFS, DR/BC has previously been identified as a top priority item and significant strides have been achieved, while acknowledging that significant efforts remain to have a complete and practical DR/BC plan in place.

EFS Accomplishments to date in regards to DR/BC include:

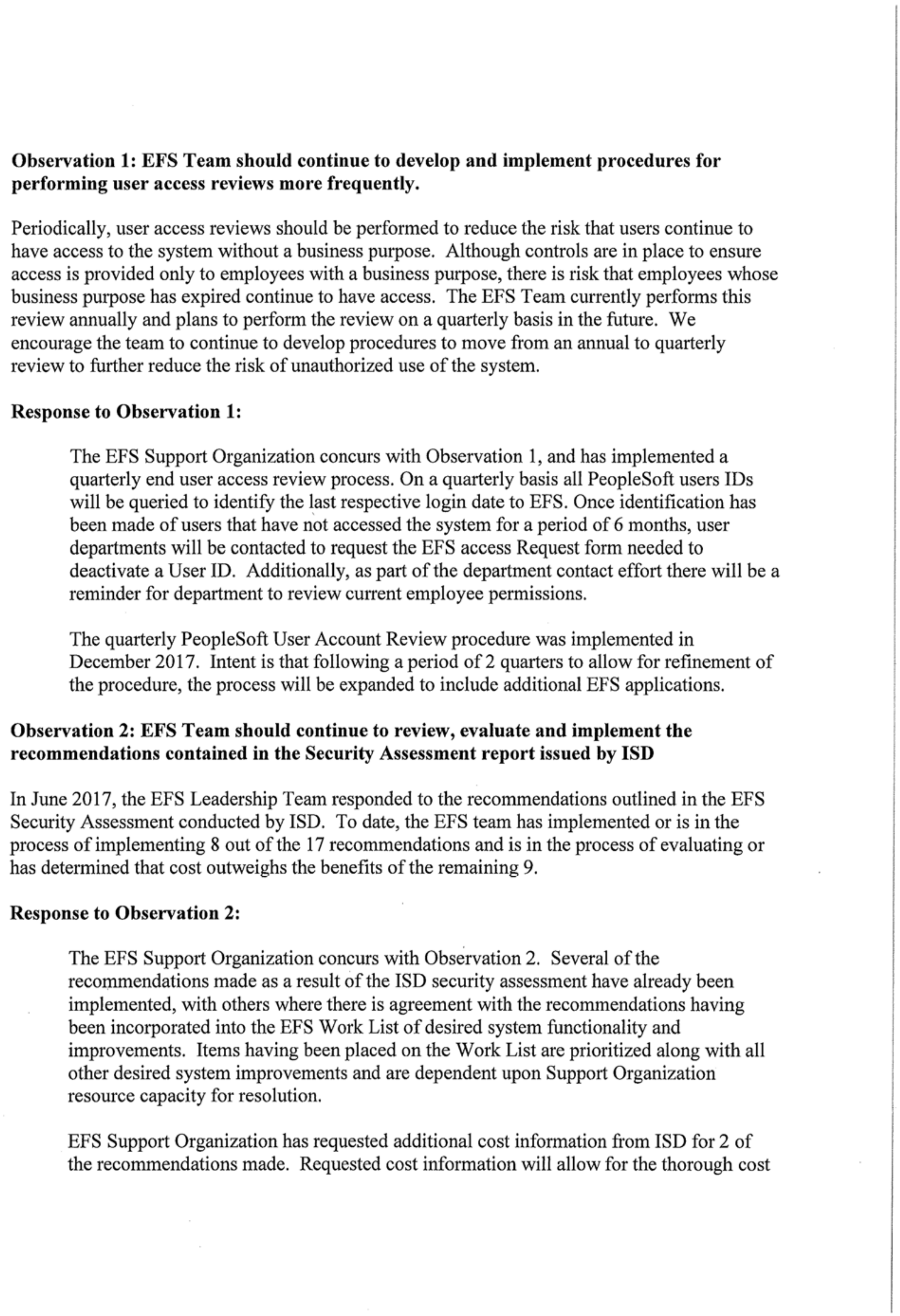
- Collaborative discussions with ISD to identify critical business needs and the desire restoration timeframe of those needs.
- Established processes to capture nightly backups of EFS production Data.
- Installation of redundant PS application and hardware at the County Emergency Operation Center (EOC).
- Identification of 3 disaster scenarios to be addressed:
    - ISD Data Center lost or degraded, other county buildings lost.
    - ISD Data Center functioning but staff cannot approach.
    - Loss of Data Center and other county buildings.
- As a direct result of the recent wildfires, established a presence on the Microsoft Azure cloud.
- Establishment of working group, consisting of ACTTC and Information Systems Department (ISD) staff, to develop and expand EFS DR/BC.

Continuing/additional efforts include:

- Test the process of restoring backups within the Azure cloud as an offsite disaster recovery environment.
- Re-review of critical functions and applications to determine:
    - Recovery Time Objective – how soon application(s) to be restored.
    - Recovery Point Objective – how old can the data be when it is restored.
- Review of server requirements for the application.
- Development of cost forecasts for the identified disaster scenarios
- Development and deployment of DR/BC plan to address all disaster scenarios that are effective, efficient and economically feasible.
- Performance of annual testing of developed DR/BC plan(s).

DR/BC is an acknowledged critical need of the ACTTC, and focused attention will be provided to EFS, as well as all other ACTTC administered IT systems, moving forward.

Appendix B: Management Responses



Observation 1: EFS Team should continue to develop and implement procedures for performing user access reviews more frequently.

Periodically, user access reviews should be performed to reduce the risk that users continue to have access to the system without a business purpose. Although controls are in place to ensure access is provided only to employees with a business purpose, there is risk that employees whose business purpose has expired continue to have access. The EFS Team currently performs this review annually and plans to perform the review on a quarterly basis in the future. We encourage the team to continue to develop procedures to move from an annual to quarterly review to further reduce the risk of unauthorized use of the system.

Response to Observation 1:

The EFS Support Organization concurs with Observation 1, and has implemented a quarterly end user access review process. On a quarterly basis all PeopleSoft users IDs will be queried to identify the last respective login date to EFS. Once identification has been made of users that have not accessed the system for a period of 6 months, user departments will be contacted to request the EFS access Request form needed to deactivate a User ID. Additionally, as part of the department contact effort there will be a reminder for department to review current employee permissions.

The quarterly PeopleSoft User Account Review procedure was implemented in December 2017. Intent is that following a period of 2 quarters to allow for refinement of the procedure, the process will be expanded to include additional EFS applications.

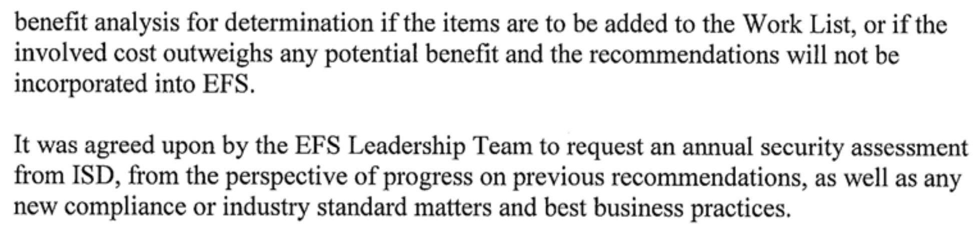
Observation 2: EFS Team should continue to review, evaluate and implement the recommendations contained in the Security Assessment report issued by ISD

In June 2017, the EFS Leadership Team responded to the recommendations outlined in the EFS Security Assessment conducted by ISD. To date, the EFS team has implemented or is in the process of implementing 8 out of the 17 recommendations and is in the process of evaluating or has determined that cost outweighs the benefits of the remaining 9.

Response to Observation 2:

The EFS Support Organization concurs with Observation 2. Several of the recommendations made as a result of the ISD security assessment have already been implemented, with others where there is agreement with the recommendations having been incorporated into the EFS Work List of desired system functionality and improvements. Items having been placed on the Work List are prioritized along with all other desired system improvements and are dependent upon Support Organization resource capacity for resolution.

EFS Support Organization has requested additional cost information from ISD for 2 of the recommendations made. Requested cost information will allow for the thorough cost



benefit analysis for determination if the items are to be added to the Work List, or if the involved cost outweighs any potential benefit and the recommendations will not be incorporated into EFS.

It was agreed upon by the EFS Leadership Team to request an annual security assessment from ISD, from the perspective of progress on previous recommendations, as well as any new compliance or industry standard matters and best business practices.