

**ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM
2223 E. WELLINGTON AVENUE, SUITE 100
SANTA ANA, CALIFORNIA**

**AUDIT COMMITTEE MEETING
September 24, 2019
2:30 P.m.**

Members of the Committee
Frank Eley, Chair
Charles Packard, Vice Chair
Jeremy Vallone
Shari Freidenrich

AGENDA

This agenda contains a brief general description of each item to be considered. The Committee may take action on any item included in the agenda; however, except as otherwise provided by law, no action shall be taken on any item not appearing on the agenda. The Committee may consider matters included on the agenda in any order, and not necessarily in the order listed.

PUBLIC COMMENT

At this time, members of the public may comment on (1) matters not included on the agenda, provided that the matter is within the subject matter jurisdiction of the Committee; and (2) any matter appearing on the Consent Agenda. **Persons wishing to provide public comment at this time should fill out a speaker card located on the counter at the back of the room and deposit it in the Recording Secretary's inbox on the wall near the middle of the room.** When addressing the Committee, please state your name for the record prior to providing your comments. Speakers will be limited to three (3) minutes.

In addition, public comment on matters listed on this agenda will be taken at the time the item is addressed.

CONSENT AGENDA

C-1 APPROVE AUDIT COMMITTEE MEETING MINUTES

Audit Committee Meeting Minutes

June 6, 2019

ACTION ITEMS

NOTE: Public comment on matters listed in this agenda will be taken at the time the item is addressed, prior to the Committee's discussion of the item. **Persons wishing to provide public comment at this time should fill out a speaker card located on the counter at the back of the room and deposit it in the Recording Secretary's inbox on the wall near the middle of the room.**

A-1 INDIVIDUAL ACTION ON ANY ITEM TRAILED FROM THE CONSENT AGENDA

A-2 AUDIT OF BUSINESS CONTINUITY AND DISASTER RECOVERY

Presentation by David Kim, Director of Internal Audit

Recommendation: Receive and file.

A-3 HOTLINE UPDATE

Presentation by David Kim, Director of Internal Audit

Recommendation: Receive and file.

INFORMATION ITEMS

I-1 STATUS UPDATE OF 2019 AUDIT PLAN

Written Report

CLOSED SESSION

A. PUBLIC EMPLOYEE PERFORMANCE EVALUATION (GOVERNMENT CODE §54957(b))

Title: Director of Internal Audit

Adjourn pursuant to Government Code section 54957(b) to evaluate the performance of the Director of Internal Audit

Recommendation: Take appropriate action.

COMMITTEE MEMBER COMMENTS

CHIEF EXECUTIVE OFFICER/STAFF COMMENTS

COUNSEL COMMENTS

ADJOURNMENT

NOTICE OF NEXT MEETINGS

DISABILITY COMMITTEE MEETING

October 3, 2019

10:00 A.M.

ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM

2223 E. WELLINGTON AVENUE, SUITE 100

SANTA ANA, CA 92701

OCERS BUDGET WORKSHOP

October 17, 2019

9:00 A.M.

ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM

2223 E. WELLINGTON AVENUE, SUITE 100

SANTA ANA, CA 92701

REGULAR BOARD MEETING

October 21, 2019

9:00 A.M.

ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM

2223 E. WELLINGTON AVENUE, SUITE 100

SANTA ANA, CA 92701

All supporting documentation is available for public review in the retirement office during regular business hours, 8:00 a.m. – 5:00 p.m., Monday through Thursday and 8:00 a.m. – 4:30 p.m. on Friday.

It is OCERS' intention to comply with the Americans with Disabilities Act ("ADA") in all respects. If, as an attendee or participant at this meeting, you will need any special assistance beyond that normally provided, OCERS will attempt to accommodate your needs in a reasonable manner. Please contact OCERS via email at adminsupport@ocers.org or call 714-558-6200 as soon as possible prior to the meeting to tell us about your needs and to determine if accommodation is feasible. We would appreciate at least 48 hours notice, if possible. Please also advise us if you plan to attend meetings on a regular basis.

C-1

ORANGE COUNTY EMPLOYEES RETIREMENT SYSTEM

**BOARD OF RETIREMENT
2223 WELLINGTON AVENUE, SUITE 100
SANTA ANA, CA 92701**

AUDIT COMMITTEE MEETING

June 6, 2019

1:00 p.m.

Members of the Committee

Frank Eley, Chair

Charles Packard, Vice Chair

Jeremy Vallone

Shari Freidenrich

MINUTES

OPEN SESSION

The Chair called the meeting to order at 1:09 p.m.

Attendance was as follows:

Committee Members: Frank Eley, Chair; Charles Packard, Vice Chair; Jeremy Vallone; Shari Freidenrich

Staff: David Kim, Director of Internal Audit; Brenda Shott, Assistant CEO of Internal Operations; Suzanne Jenike, Assistant CEO External Operations; Tracy Bowman, Director of Finance; Mark Adviento, Internal Auditor; Sonal Sharma, Recording Secretary; Anthony Beltran, Audio Visual Technician.

PUBLIC COMMENT

None.

CONSENT AGENDA

C-1 APPROVE AUDIT COMMITTEE MINUTES

Audit Committee Meeting Minutes

March 26, 2019

A **motion** was made by Mr. Packard, **seconded** by Mr. Vallone to approve the minutes.

ACTION ITEMS

A-2 2018 FINANCIAL STATEMENT AUDIT

Presentation by Linda Hurley and Amy Chiang, Macias Gini & O'Connell

Recommendations:

1. Approve OCERS' audited financial statements for the year ended December 31, 2018;

2. Direct staff to finalize OCERS' 2018 Comprehensive Annual Financial Report (CAFR);
3. Approve the Governmental Accounting Standards Board (GASB) Statement 67 Actuarial Valuation as of December 31, 2018; and
4. Receive and file Macias, Gini & O'Connell LLP's (MGO) "OCERS' Report to the Audit Committee for the Year Ended December 31, 2018" and its "Independent Auditor's Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*."

A **motion** was made by Mr. Packard, **seconded** by Ms. Freidenrich to approve staff recommendation.

A-3 GASB 68 VALUATION AND AUDIT REPORT

Presentation by Brenda Shott, Assistant CEO of Internal Operations

Recommendations:

1. Approve OCERS' audited Schedule of Allocated Pension Amounts by Employer as of and for the Year Ended December 31, 2018; and
2. Approve the Governmental Accounting Standards Board (GASB) Statement 68 Actuarial Valuation as of December 31, 2018 for distribution to employers.

A **motion** was made by Mr. Packard, **seconded** by Ms. Freidenrich to approve staff recommendation.

A-4 AUDIT OF EMPLOYER AND EMPLOYEE CONTRIBUTIONS ACCOUNTING

Presentation by David Kim, Director of Internal Audit and Mark Adviento, Internal Auditor

Recommendation: Receive and file.

A **motion** was made by Mr. Packard, **seconded** by Mr. Vallone to approve staff recommendation.

A-5 MANAGEMENT ACTION PLAN VERIFICATION

Presentation by David Kim, Director of Internal Audit

Recommendation: Receive and file.

A **motion** was made by Mr. Packard, **seconded** by Mr. Vallone to approve staff recommendation.

A-6 HOTLINE UPDATE

Presentation by David Kim, Director of Internal Audit

Recommendation: Receive and file.

A **motion** was made by Mr. Packard, **seconded** by Mr. Vallone to approve staff recommendation.

INFORMATION ITEMS

I-1 STATUS UPDATE OF 2019 AUDIT PLAN

Written Report

I-2 TRAVEL REPORT - LACERA

Written Report

******* END OF OPEN SESSION AGENDA *******

CLOSED SESSION 3:00

E-1 THREAT TO PUBLIC SERVICES OR FACILITIES (GOVERNMENT CODE SECTION 54957)

Adjourn into Closed Session pursuant to Government Code section 54957 to consult with *Steve Delaney, CEO, Brenda Shott, Asst. CEO; Matthew Eakin, Director of Cyber Security; Jenny Sadoski, Director of Information Technology; Jon Gossard, Information Security Manager; and Gina M. Ratto, General Counsel*

Recommendation: Take appropriate action.

******* END OF CLOSED SESSION AGENDA *******

OPEN SESSION

The Committee recessed into open session. No reportable action was taken.

COMMITTEE MEMBER COMMENTS

None.

CHIEF EXECUTIVE OFFICER/STAFF COMMENTS

None.

COUNSEL COMMENTS

None.

ADJOURNMENT

The Chair adjourned the meeting at 3:41pm.

Audit Committee Meeting
June 6, 2019

Submitted by:

Approved by:

Steve Delaney
Secretary to the Board

Frank Eley
Chair

A-2



Memorandum

DATE: September 24, 2019
TO: Members of the Audit Committee
FROM: D. Kim, Director of Internal Audit
SUBJECT: **AUDIT REPORT – BUSINESS CONTINUITY AND DISASTER RECOVERY**

Recommendation

Receive and file.

Background/Discussion

As per the 2019 Audit Plan, Internal Audit performed an audit of OCERS' Internal Controls over the Business Continuity and Disaster Recovery program.

There were eight observations directed towards OCERS management. Further details on the observations and management's responses are provided in the audit report.

The full audit report is attached.



Audit of Business Continuity and Disaster Recovery

Report Date: September 24, 2019

Internal Audit Department

David Kim, Director of Internal Audit

Mark Adviento, Internal Auditor

OCERS Internal Audit
Audit of Business Continuity and Disaster Recovery
September 24, 2019

Table of Contents

Audit Objective and Scope.....	1
Conclusion and Executive Summary.....	1
Background.....	1
Observation Summary.....	2
Observation Details.....	5

Audit Objective and Scope

The objective of this audit was to provide an independent review of the controls over the Business Continuity and Disaster Recovery (BCDR) process to ensure the effectiveness of the preparedness efforts as well as the ongoing management of the BCDR program.

The scope of the audit included the overall program governance, ongoing program management and testing of the BCDR program.

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing issued by the International Internal Audit Standards Board.

Conclusion / Executive Summary

Opinion: *Opportunities for Improvement*

Overall, controls are in place to ensure the preparedness of the BCDR is effective as well as the ongoing management of the program. The BCDR program was updated in 2015 and continues to develop as the program matures/evolves. There were eight Important Observations which included the need to formally document the approval of the OCERS' Business Continuity Policy document which has been in existence since 2015. In addition, formalizing the standard operating procedure as well as the recovery testing of dependent applications with the business owners is necessary to ensure the restoration of operations is meeting management's expectations. We also noted opportunities to strengthen the organizational preparedness for the BCDR program at the department level.

Background

The business continuity and disaster recovery program addresses OCERS' operations at OCERS' headquarters and focuses on OCERS' key business capabilities. The purpose of the OCERS Business Continuity Program is to identify the resources needed to meet stakeholder expectations, understand risks that could influence resource availability, and develop strategies that reasonably mitigate or manage risk. The OCERS' Business Continuity Plan was updated in 2014 from the earlier iteration dated September 1994. OCERS had contracted Avalution in 2015 to assist with the development of the BCDR program, BCDR application (Catalyst) and ongoing management. A Crisis Management Team (CMT) comprised of OCERS employees was established to oversee the BCDR program, along with a designated Continuity Program Manager to execute the program tasks. A Business Impact Analysis (BIA) was performed with Avalution and documented to determine business continuity requirements, define risk mitigation and recovery responses. The outcome of the analysis was used to identify strategies to limit the impact of a disruptive incident and enable a timely recovery. The documented program consists

of activities that enable OCERS to respond to and recover from disruptive incidents at both the entity and department levels. As part of the BCDR program management, regularly scheduled tabletop training exercises are conducted to ensure employees understand their respective roles within the response and recovery effort; validate planned strategies, tools, and resources; and identify improvement opportunities.

Important Observations

- ▶ **OCERS Business Continuity Policy document has existed since 2015 but the documentation of the approvals were not formalized.** The OCERS Business Continuity Policy maintained in Catalyst, the BCDR system of record, is in draft version, last revised August 20, 2015. The Crisis Management Team (CMT) had reviewed the Policy but did not formally document the approval. By not formalizing the approval, the BCDR program may lack the necessary oversight to fulfill the objectives of the program. In response to our observation, the CMT will review and retitle the document as the OCERS Business Continuity Program. The OCERS CEO will formally approve the updated document. Furthermore, staff will recommend a change to the CEO Charter to delegate the management of the Business Continuity Program to the CEO.
- ▶ **The Business Continuity Program Standard Operating Procedures document has existed since 2015 but the documentation of the approvals by the Crisis Management Team were not formalized.** The OCERS Business Continuity Program Standard Operating Procedures (SOP) document maintained in Catalyst is in draft version, last revised on September 23, 2015. The CMT had reviewed the document but did not formally document the approval. By not formalizing the approval, the CMT may not consistently execute all the key elements of the BCDR program. In response to our observation, the CMT will review and update, as necessary, the SOP and will formally document the approval.
- ▶ **A formal process involving critical OCERS stakeholders is not in place to test the recovery of dependent IT applications.** The recovery testing of dependent servers and applications tested by IT does not include the business process owners. Without the participation of the business process owners, OCERS cannot confirm the data recovery objectives have been met in a complete and accurate manner. In response to our observation, IT will formalize a new Business Continuity and Disaster Recovery test plan that will include test activities, confirmation, and sign-off by the various business units within OCERS.
- ▶ **The tabletop exercise did not fully validate the organization's preparedness at an entity or department level in the event of a disaster.** Internal Audit observed during the Q3 2019 tabletop exercise a high level of collaboration among the CMT however, the participants did not demonstrate explicit referral to the Crisis Management Plan or Recovery Plans, either at the entity or the department level. By relying upon an individual or subset of individuals instead of referring to the agreed upon procedures, the CMT did not demonstrate the level of preparedness that is needed to restore operational and IT processes in the event of a disruptive incident. In response to our observation, the CMT Coordinator will reiterate the importance of referring to the appropriate procedures during the exercise. Additionally, the CMT will expand scenarios to functional exercises that will test the reliance upon the Crisis Management Plan and Department Recovery Plans.

- ▶ **Management personnel are not consistently updating the relevant information in the Business Impact Analysis and Department Recovery Plan documents in a timely manner.** During our review, Internal Audit noted that the contact information for 4 of the 11 BIAs and the recovery phase information for 3 of the 7 Department Recovery Plans were not updated timely. The updates were eventually made during the BCDR refresh meetings in July 2019. Updates not made to the BIA and Department Recovery Plans in a timely manner may lead to inaccurate information during a time of disaster for the respective department. In response to our observation, the CMT Leader will remind the plan owners on a quarterly basis to update the required documentation when changes to processes, personnel or technology have occurred. The CMT Leader will also work with Administrative Services to add worksteps to the off-boarding and on-boarding processes to update the BCDR documentation based on the termination or hiring of an employee.

- ▶ **Recovery procedures for dependent IT applications are not documented in the recovery plans.** We noted that the IT recovery plans do not include detailed procedures for recovery but rely on the institutional knowledge of the IT recovery team. However, if a disaster were to impact the IT recovery team, the ability to restore dependent applications in a timely manner would be compromised. In response to our observation, IT will document the recovery procedures for the dependent systems and will store the documentation in Catalyst.

- ▶ **The identification of alternative facility locations has not been formally documented and approved in the BCDR system.** In our review, we noted that there are two separate documents in Catalyst referenced for alternative facilities, both of which were noted as draft. Without an approved document to formally identify the alternative facility locations, OCERS may not be able to resume operations within the required timeframes. In response to our observation, the CMT Coordinator team will continue to finalize the alternative facilities documentation, which includes establishing a formal agreement with the County of Orange for use of their facilities.

- ▶ **Key members of the Crisis Management Team (CMT) are not consistently taking the assigned electronic resources when traveling from the office.** We noted laptops belonging to two members of the CMT remained in the office on two separate days while the respective CMT members had left the office for the day or were away on travel. While CMT members have noted they travel with their cellphones, they may not be able to readily access critical information or applications in the event of a disaster without their laptops. In response to our observation, the CMT Leader will regularly remind the CMT members the importance of being prepared with the necessary resources available in the event of a disaster.

Copies to:

S. Delaney
S. Jenike
M. Murphy
G. Ratto
B. Shott

A. Bercaru
T. Bowman
S. Chary
M. Cortez
J. Doezie
M. Eakin

J. Gossard
C. Hockless
R. Kinsler
J. Lara
J. Sadoski
M. Wozniuk
Audit Committee Members

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p align="center">Important Observations</p>	
<p>1. OCERS Business Continuity Policy document has existed since 2015 but the documentation of the approvals were not formalized.</p> <p>The OCERS Business Continuity Policy maintained in Catalyst, the business continuity and disaster recovery (BCDR) system of record, is in draft version, last revised August 20, 2015.</p> <p>The OCERS Business Continuity Program (Program) is an enterprise-wide activity to develop strategies that reasonably mitigate or manage unforeseen risks that could have a disruptive impact on resource availability. The Program requires the participation from all critical functions at OCERS to meet the stakeholder expectations. The Business Continuity Policy documents the mission, purpose, objectives, and roles for the Program Without a formally approved policy, the Program may lack the necessary oversight to fulfill the objectives of the Program.</p> <p>The risks are mitigated by the active participation of all the current Senior Executive team in the quarterly reviews and bi-annual exercises of the BCDR program. However, in order to ensure the continued sustainability of the Program’s mission and objectives, the policy should be formally reviewed and approved on a regular cadence by the appropriate personnel.</p>	<p>Management Action Plan: We believe that the current document titled “OCERS Business Continuity Policy” would be more accurately described as a program document. As such, our plan is to retitle the document to be OCERS Business Continuity Program and review it with the CMT making updates as deemed appropriate. The Chief Executive Office will then formally approve the updated document. The updated document will be reviewed every three years for necessary changes.</p> <p>As an extension to this observation, staff will also recommend to the Board of Retirement a change to the CEO Charter the next time the Charter is due for a review. The change will be to specifically delegate to the CEO the duty of implementing, testing and maintaining a Business Continuity Program.</p> <p>Management Action Plan Responsible Party: Brenda Shott, Assistant CEO, Finance and Internal Operations</p> <p>Completion Date: October 29, 2019</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>Risk: The OCERS Business Continuity Program may lack the necessary oversight to fulfill the objectives of the Program.</p>	
<p>2. The Business Continuity Program Standard Operating Procedures document has existed since 2015 but the documentation of the approvals by the Crisis Management Team were not formalized.</p> <p>The OCERS Business Continuity Program Standard Operating Procedures (SOP) document maintained in Catalyst, the BCDR system of record, is in draft version, last revised on September 23, 2015.</p> <p>The SOP document contains the detailed program objectives, scope, limitations and expectations of the Business Continuity Program that were initially outlined in the Business Continuity Policy. The SOP document provides guidance on the key elements of the Program and sets standards for the business continuity activities to be performed by OCERS personnel. Some of the key elements noted in the SOP document are Program Objectives, Business Continuity Procedures, Stakeholder Awareness along with Program Element and Activity Performance Schedule. Without the proper review and approval of the SOP document, the Crisis Management Team may not consistently address all the key elements and activities of the Business Continuity Program on a regular basis.</p>	<p>Management Action Plan: We concur with the observation and will formalize the approval of the document.</p> <p>Management Action Plan Responsible Party: Brenda Shott, Assistant CEO, Finance and Internal Operations</p> <p>Completion Date: October 29, 2019</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>The mitigating factors that addresses the risk is the institutional knowledge of the Business Continuity Coordinator and Alternate Business Continuity Coordinator. However, the reliance upon personnel to maintain the continued operational effectiveness of the Program without documented guidance is not sustainable, considering the nature of risks this program is intended to mitigate.</p> <p>Risk: The Crisis Management Team may not consistently execute all the key elements and activities of the Business Continuity Program on a regular basis.</p>	
<p>3. A formal process involving critical OCERS stakeholders is not in place to test the recovery of dependent IT applications.</p> <p>The disaster recovery of dependent applications is designed to restore the target systems OCERS relies upon to resume operations. To derive the most value, the test plan should be designed to examine the selected element(s) against explicit test objectives and success criteria. The use of test objectives and success criteria enable the effectiveness of each system element and the overall plan to be assessed. The test plan should include a schedule detailing the time frames for each test and test participants. The participants should include personnel representing the various departments within OCERS to confirm data recovery objectives have been met.</p>	<p>Management Action Plan: OCERS IT will formalize and adopt a new Business Continuity and Disaster Recovery test plan that will include test activities, confirmation, and sign-off by the various business units within OCERS.</p> <p>Management Action Plan Responsible Party: Jenny Sadoski, Director of Information Technology</p> <p>Completion Date: July 31, 2020</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>Currently, IT performs informal recovery testing of various servers and applications to ensure the technical resources can be restored in a disaster. IT did perform a system fail-over test of Dynamics with OCERS Finance personnel in Q1 2019. However, business process owners should work with IT during the recovery testing in a formalized manner to confirm that the data recovery objectives have been met, as they are in the best position to validate the information. Additionally, the joint testing would clarify management's expectations of the data recovery objective for the targeted systems in preparation for a disaster.</p> <p>Risk: Data recovery needed to restore operations may not meet management's expectations.</p>	
<p>4. The tabletop exercise did not fully validate the organization's preparedness at an entity or department level in the event of a disaster.</p> <p>Business Continuity exercises allow personnel with operational responsibilities to validate their operational and IT readiness for emergencies by performing their duties in a test case scenario. While tabletop exercises have been performed over the past four years, as the BCDR program continues to mature, the tabletop exercises do not consistently reinforce the training the identified personnel received on their roles and responsibilities of the recovery plans at the department level.</p>	<p>Management Action Plan: We believe the program is ready to enhance future exercises by including more functional testing. As an example, during our July 2019 tabletop, a component of the Finance team was asked to work from home in order to test their connectivity and functionality. In future exercises, we will expand the scenarios to encompass various departments within the organization such that over time, all departments with a recovery plan will have participated in a functional exercise. For upcoming exercises, we will create scenarios which allow us to include departments which have not yet participated in an exercise.</p> <p>We have added an item to the October 2019 Crisis Management Team meeting to discuss timing of the expansion of functional testing efforts as well as the importance of referring to the Crisis Management Plan and Department Recovery Plans during exercises. Our recommendation will be to conduct IT testing as part of our January exercises and deeper functional testing as part of our July exercises.</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>Internal Audit had observed during the Q3 2019 tabletop exercise that there was a high level of collaboration among the CMT however, the participants did not demonstrate explicit referral to the Crisis Management Plan or Recovery Plans, either at the entity or the department level. These documents provide the guidance to team members on the specific procedures that are involved to restore operational activities in a disaster situation. Instead, the CMT deferred to one of the CMT leaders who was familiar with the process rather than defaulting to the agreed upon procedures. The risk is conditioning the CMT to rely upon a specific person or subset of people instead of the Crisis Management Plan or Recovery Plans.</p> <p>Furthermore, the BCDR exercises were limited to tabletop exercises. Introducing functional exercises to the BCDR program would enhance the operational readiness training of the CMT. Functional exercises are designed to exercise specific team members, procedures, and resources involved in one or more functional aspects of a test scenario (e.g., communications, emergency notifications, IT equipment set-up). These types of exercises would require the participants to implement manual workarounds and eventually reconnect to the IT systems once restored. Personnel would test their capability to perform their operational tasks in an off-site scenario (e.g. answer phones, issue payments) relying upon their training and the BCDR documentation. It has been noted that there have been elements of a functional exercise introduced in</p>	<p>Management Action Plan Responsible Party: Jon Gossard, Information Security Manager and Jim Doezie, Contracts Administrator</p> <p>Completion Date: Discuss timing of the expansion of functional testing efforts - October 29, 2019</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>the last tabletop exercise (Q3 2019), and there are plans to expand the scope of future testing.</p> <p>Risk: Personnel would not be able to restore operational and IT activities during a disaster situation in a timely manner.</p>	
<p>5. Management personnel are not consistently updating the relevant information in the Business Impact Analysis and Department Recovery Plan documents in a timely manner.</p> <p>The Business Impact Analysis (BIA) document is a management tool designed to determine the impact of any disruption of activities that support the organization's key business capabilities. The BIAs include key information such as the activities for each department, applications used in the department, supplier dependencies and other OCERS departments dependencies. The Department Recovery Plans documents the defined roles and responsibilities for personnel that have authority during and following a disruptive incident. The Department Recovery Plans provide details on strategic and operational options for responding to the disruption. Representatives from each of the departments are designated as Plan Owners who are responsible for participating in the development of both the BIA and the Department Recovery Plans. Additionally, the Plan Owners are responsible for maintaining the relevant information within the BIA and Department Recovery Plans.</p>	<p>Management Action Plan: The CMT Leader, OCERS CEO, will remind the CMT at least two weeks prior to the quarterly Business Continuity meetings to update the appropriate Business Continuity documents to reflect any changes in personnel, technology or vendors since the last meeting. Additionally, the CMT Leader will add as a standing agenda item for the quarterly meetings a reminder that the CMT should update the appropriate Business Continuity documents. The plan owners will update the necessary documents based on the reminder at least on a quarterly basis.</p> <p>The CMT Leader will also work with Administrative Services to add a workstep in the off-boarding and on-boarding processes for the plan owners to assess the organizational impact of the terminated or new employee to the Business Continuity documentation. Based on the assessment, the plan owner will update the documentation accordingly.</p> <p>Management Action Plan Responsible Party: Steve Delaney, CEO</p> <p>Completion Date: October 29, 2019</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>During our review, we noted that the contact information for 4 of the 11 BIAs continued to reference a Finance Manager that had retired in February 2019. Additionally, 3 of the 11 BIAs continued to reference an Information Security Manager as the IT contact after he had transitioned out of the role in January 2019. Three of the seven Department Recovery Plans were not updated since the prior year refresh period although changes were required. The updates were eventually made during the BCDR Refresh held in July 2019.</p> <p>Risk: Updates not made to the BIA and Department Recovery Plans in a timely manner may lead to inaccurate information during a time of disaster for the respective department.</p>	
<p>6. Recovery procedures for dependent IT applications are not documented in the recovery plans.</p> <p>To facilitate Recovery Phase operations, detailed procedures to restore the information system or components to a known state should be documented. Recovery procedures should be written in a straightforward manner. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted.</p> <p>We noted that the IT recovery plans do not include detailed procedures for recovery but rely on the institutional knowledge of the IT recovery team. However, if a disaster impacts the IT recovery team,</p>	<p>Management Action Plan: End User documents are being developed for the purpose of providing recovery instructions to the crisis management team, in the event IT staff are not available in the event of an emergency. The documents will provide simple easy to follow instructions on how to failover and/or recover sites or systems in the event of a technology failure. These documents will be included in OCERS IT Backup and Recovery test plan stored in Catalyst to ensure procedures are complete and can be followed by non- IT staff.</p> <p>Management Action Plan Responsible Party: Jenny Sadoski, Director of Information Technology</p> <p>Completion Date: April 30, 2020</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>the ability to restore dependent applications would be compromised.</p> <p>Risk: Dependent IT applications are not restored in a timely manner.</p>	
<p>7. The identification of alternative facility locations has not been formally documented and approved in the BCDR system.</p> <p>Alternate facilities provide a location for an organization to resume system operations in the event of a catastrophic event that disables or destroys the systems primary facility. Through the Business Impact Analysis (BIA) annual updates, it was noted that OCERS would eventually need to have a location for a minimum of 11 staff after four days of a disaster and a location to house a minimum of 34 staff five days after an incident. If the OCERS headquarters building was unavailable during those timeframes, staff would need an alternative facility to resume operations.</p> <p>In our review, we noted that there are two separate documents referenced for alternative facilities, both of which were noted as draft. In discussions with the Business Continuity Coordinator, it was noted that they are in the process of establishing a formal agreement with the County of Orange for use of their facilities in a disaster. Additionally, OCERS has other workspace arrangements that may be used, if necessary, such as a mobile workspace. However,</p>	<p>Management Action Plan: The Business Continuity Coordinator team is currently working with the County of Orange to formalize an agreement to use County facilities as an alternate workspace location in the event of a localized disaster at OCERS headquarters. The County requested OCERS to complete a questionnaire, which was completed and sent back to the County on August 8, 2019. The most recent conversations with the County occurred on August 21, 2019; we will schedule a follow-up call with County representatives in the very near future.</p> <p>Once the agreement is formalized, all program documentation will be updated to include the alternate workspace site information and an action item to review the alternate workspace location on an annual basis will be created. This action item will serve to ensure that the alternate workspace location is still viable. The BC Coordinator team will continue to refine the alternate workspace options for additional scenarios. In addition, the BC Coordinators will create a schedule detailing space needs over time.</p> <p>Management Action Plan Responsible Party: Jon Gossard, Information Security Manager and Jim Doezie, Contracts Administrator</p> <p>Completion Date: Follow-up call with the County on the status of the alternate workspace agreement – September 26, 2019</p>

Observation Details	Management Action Plan (MAP) /MAP Responsible Party / Completion Date
<p>without an approved document to formally identify the alternative facility locations, OCERS may not be able to resume operations within the required timeframes.</p> <p>Risk: OCERS may not be able quickly identify an alternative facility to resume operations in a timely manner.</p>	
<p>8. Key members of the Crisis Management Team (CMT) are not consistently taking the assigned electronic resources when traveling from the office.</p> <p>Audit staff performed a spot check on two separate days and found that two key members of the CMT left the office without their laptops on both occasions. The laptops had been identified as one of the key resource requirements in the event of a disaster in the Business Impact Analysis documents. CMT members have noted that they frequently travel with their cellphones, which has the Catalyst application as well as access to email. However, the laptops provide additional capabilities that is not easily accessible on cellphones, such as access to SharePoint or other OCERS' applications.</p> <p>Risk: Members of the Crisis Management Team may not be able to readily access critical information or applications during a disaster.</p>	<p>Management Action Plan: The CMT Leader, OCERS CEO, will remind the CMT at the quarterly Business Continuity meetings of the importance of taking the necessary resources (laptops) when traveling away from the office.</p> <p>Management Action Plan Responsible Party: Steve Delaney, CEO</p> <p>Completion Date: October 29, 2019</p>

Categories of Observations (Control Exceptions):

Priority Observations:

These are observation(s) that represent critical exceptions to the audit objective(s) and/or business goals. Such conditions may involve either actual or potential large dollar errors or be of such a nature as to compromise OCERS' reputation or integrity. Management is expected to address Priority Observations brought to its attention immediately.

Important Observations:

These items are important to the process owner and they do impact the control environment and/or could be observations for improving the efficiency and/or effectiveness of OCERS' operations. Management is expected to address within six to twelve months.

Management's Responsibility for Internal Control

Management has primary responsibility for establishing and maintaining the internal control system. All levels of management must be involved in assessing and strengthening internal controls." Control systems shall be continuously evaluated by Management and weaknesses, when detected, must be promptly corrected. The criteria for evaluating an entity's internal control structure are the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework. Our Internal Control Audit enhances and complements, but does not substitute for department management's continuing emphasis on control activities and self-assessment of control risks.

Internal Control Limitations

Because of inherent limitations in any system of internal control, errors or irregularities may nevertheless occur and not be detected. Specific examples of limitations include, but are not limited to, resource constraints, unintentional errors, management override, circumvention by collusion, and poor judgment. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or the degree of compliance with the procedures may deteriorate. Accordingly, our audit would not necessarily disclose all weaknesses in the department's operating procedures, accounting practices, and compliance with OCERS' policies.

Audit Report Opinions:

Satisfactory:

No issues or a limited number of “Important Observations”.

Opportunities for Improvement:

Multiple issues classified as “Important Observations” with limited or no “Priority Observations”.

Inadequate:

Usually rendered when multiple issues are classified as “Priority”, together with one or more other issues classified as “Important Observations”. The Priority Observations identified have a major effect on processes, plan sponsors/members, financials, and/or regulatory requirements.

A-3

Memorandum

DATE: September 24, 2019
TO: Members of the Audit Committee
FROM: David Kim, Director of Internal Audit
SUBJECT: HOTLINE UPDATE

Recommendation

Receive and file.

Background/Discussion

Internal Audit regularly updates the Audit Committee when new reports are made to the hotline.

Internal Audit received three reports from the hotline:

- June 13, 2019 – a complaint was made questioning a retired member’s disability status. Member Services reviewed the member’s file and concluded that the documentation supports the original decision for disability.
- September 10, 2019 – an update to a complaint made on May 4, 2019 regarding the eligibility of a specialty pay item of an OCFA member. Upon further review, OCFA has determined not to take further action with the employee. OCFA issued a side letter to clarify any ambiguity related to this specialty pay item in the MOU.

Submitted by:



David Kim
Director of Internal Audit

I-1

Memorandum

DATE: September 24, 2019
TO: Members of the Audit Committee
FROM: D. Kim, Director of Internal Audit
SUBJECT: STATUS OF 2019 INTERNAL AUDIT PLAN

Written Report

Background/Discussion

Following is a brief description of status of in-progress projects for the 2019 audit plan.

- **Benefits and Lump Sum Accounting:** Testing is near complete. The objective of the audit is to review Finance Division controls that ensure the recording of benefit payments to the GL are complete, accurate and timely.
- **IT Audit Program:** Testing with the IT Division and co-sourced IT Auditor are underway. The consultant will develop the Information Technology Risk Assessment and long term IT Audit Program plus test OCERS' IT General Controls under the direction of Internal Audit.
- **Management's Risk and Control Matrices:** Internal Audit is continuing to work with management to update management's inventory of key business objectives, associated risks, and management's controls to mitigate these risks.
- **Management Action Plan Verification:** Ongoing review of prior action plans to confirm completion and perform testing of the action plans.
- **Investment Consulting Project:** Planning is underway, entrance meeting held with Investment Department to discuss agreed upon procedures.
- **Continuous Improvement Program:** Ongoing monitoring of submissions and system maintenance.