OCTA

November 12, 2014

To: Finance and Administration Committee

From: Darrell Johnson, Chief Executive Officer

Janet Sutter, Executive Director
Internal Audit Department

Subject: Performance Audit of the Orange County Transportation Authority's Continuity Plan

Overview

A performance audit of the Orange County Transportation Authority's continuity plan has been completed by the professional accounting and advisory firm, BCA Watson Rice, LLP, under contract to the Internal Audit Department. The auditors have recommended that management re-perform the business impact analysis, and update and reissue the continuity plan to address several deficiencies.

Recommendations

A. Direct staff to develop a plan to specifically address deficiencies, commit to implementation dates, and report to the Security Working Group at its next meeting.

B. Direct the Internal Audit Department to provide the Finance and Administration Committee information on the status of outstanding recommendations through quarterly updates to the Fiscal Year 2014-15 Internal Audit Plan.

C. Direct staff to return to the Finance and Administration Committee upon completion of the updated continuity plan.

Background

The purpose of a continuity plan (Plan) is to prepare an agency to resume critical functions in a timely manner following a significant emergency event. In

order to develop a Plan, an organization must first perform a business impact analysis (BIA).

In August 2010, the Federal Emergency Management Agency awarded $200,000, in Transit Security Grant Program funds for the development of a Plan for the Orange County Transportation Authority (OCTA). Transit Division staff contracted with a consultant in May 2012, to, among other tasks, perform an agency-wide BIA, develop a Plan, and perform staff training on the Plan. The BIA was completed in October 2012, training was performed in April 2013, and the Plan was delivered in May 2013.

A review of the Plan was included in the Fiscal Year 2013-14 Internal Audit Plan approved by the Board of Directors on August 12, 2013. The Internal Audit Department (Internal Audit) contracted with the professional accounting and advisory firm, BCA Watson Rice, LLP (auditors) to perform the review. The objective of the audit was to assess the adequacy and completeness of the Plan developed for OCTA. The BIA and the Plan were assessed against industry standards and, based on the auditors' professional experience, best practices in this area.

Discussion

In reviewing the BIA, the auditors found that the BIA did not comply with OCTA's Business Continuity Security Policy (Policy) or industry standards. Auditors cited a lack of prioritization of business processes, disruption scenarios and their relative likelihood and impact, and identification of the systems necessary for resumption of critical activities. While OCTA's Information Technology Department contracts with a backup site and performs testing to ensure certain applications can be brought up following a disaster, the BIA did not review these applications in conjunction with the activities identified as critical to ensure that the systems on the list are those that support the critical activities identified. In response, management advised that grant funds have been awarded to complete a Threat, Hazard Identification, and Risk Assessment project that will include an update to the BIA. While that effort is expected to take approximately 24 months to complete, management also indicated that portions of the BIA will be updated within six months.

The Plan that was produced was also not developed in compliance with Policy or industry standards. The Plan lacks detailed procedures, equipment, and systems recovery plans to ensure that functions can be resumed. The Plan also lacks consideration and integration of other related plans such as the Crisis Communications Plan and the Emergency Operations Plan. While the Plan states that it "…has been adopted by the Board of Directors…" and the

"…Chief Executive Officer has approved the Plan…," this has not occurred. The auditors noted that the consultant provided training on the Plan prior to the Plan being finalized. Employee input and comments on the draft Plan that were provided at these training sessions were never addressed or incorporated into the final document. In response, management indicated that updates to certain portions of the Plan are underway; the first update is expected to be published within six months.

Finally, the auditors noted that the identified alternate facility sites do not conform to best practices. Specifically, the Plan includes an inventory of available facilities, but lacks details of the site capabilities. As such, it is not clear whether the sites selected by individual divisions as alternate facilities would meet their needs. Also, most divisions have selected the Garden Grove Base location as their alternate facility. Whether that facility could accommodate all of these departments is also not addressed. Finally, this facility does not meet the industry standard of being far enough from OCTA's main facility.

The auditors recommended that management update the BIA and the Plan to address the weaknesses noted. In addition, the auditors recommended that management consider performing an Independent Verification and Validation to assess adequacy and completeness of the updated Plan. As noted above, management responded that efforts are underway to update certain portions of the BIA and the Plan.

At the direction of the Chairman of the Finance and Administration Committee (F&A), results of the audit were presented to the Security Working Group (SWG) for review and follow-up. The SWG directed staff to specifically address deficiencies, commit to implementation dates, and report back to the SWG at its next meeting.

As with all audit report recommendations, Internal Audit will provide F&A with information on the status of implementation of recommendations through quarterly updates to the Fiscal Year 2014-15 Internal Audit Plan. Also, staff will return to F&A upon completion of the updated Plan.

Summary

A performance audit of OCTA's Plan has been completed. The auditors have recommended that management update the BIA and the Plan to address deficiencies noted.

Attachment

A. Orange County Transportation Authority, Performance Audit of the Continuity Plan, October 3, 2014, Revised Final Report

Prepared by:

Ricco Bonelli
Senior Internal Auditor
714-560-5384

Approved by:

Janet Sutter
Executive Director, Internal Audit
714-560-5591

ATTACHMENT A

BCA Watson Rice LLP
Certified Public Accountants and Advisors

21250 Hawthorne Blvd. Suite 150
Torrance, CA 90503
www.bcawatsonrice.com

Telephone: 310.792.4640
Facsimile: 310.792.4331

ORANGE COUNTY TRANSPORTATION AUTHORITY

Performance Audit of the

Continuity Plan

October 3, 2014

REVISED FINAL REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Orange County Transportation Authority's (OCTA) Internal Audit Department contracted with BCA Watson Rice (BCAWR) on April 30, 2014 to conduct a performance audit of OCTA's Continuity Plan (Plan). While the Plan includes some useful information required for business resumption, the Business Impact Analysis (BIA), which is critical to development of an effective Plan, was incomplete and the final Plan is inadequate, as detailed in the findings of this report. We recommend that management update the BIA in accordance with OCTA policy and industry standards and then update the Plan accordingly.

This audit was a part of OCTA's Internal Audit Department's Audit Plan for FY 2013-14 and consisted of a review of OCTA's Plan for readiness and ability to recover in the event of a disaster. BCAWR conducted the performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and relevant best practices. GAGAS requires that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. BCAWR believes that the evidence obtained provides a reasonable basis for our findings and recommendations.

The primary objective of this performance audit was to assess the adequacy and completeness of OCTA's Plan. OCTA provided suggested audit steps in their Contract Task Order (CTO) proposal request. BCAWR used OCTA's suggested audit steps as the basis for developing our detailed work plan to perform this engagement. We expanded on OCTA's suggested audit steps, incorporating industry standard procedures and best practices and our professional experience and judgment to create the detailed work plan as outlined in the methodology section of this executive summary. Our review of the Plan included all data received from OCTA as a result of our request for documentation presented to OCTA.

The remainder of this page is intentionally left blank.

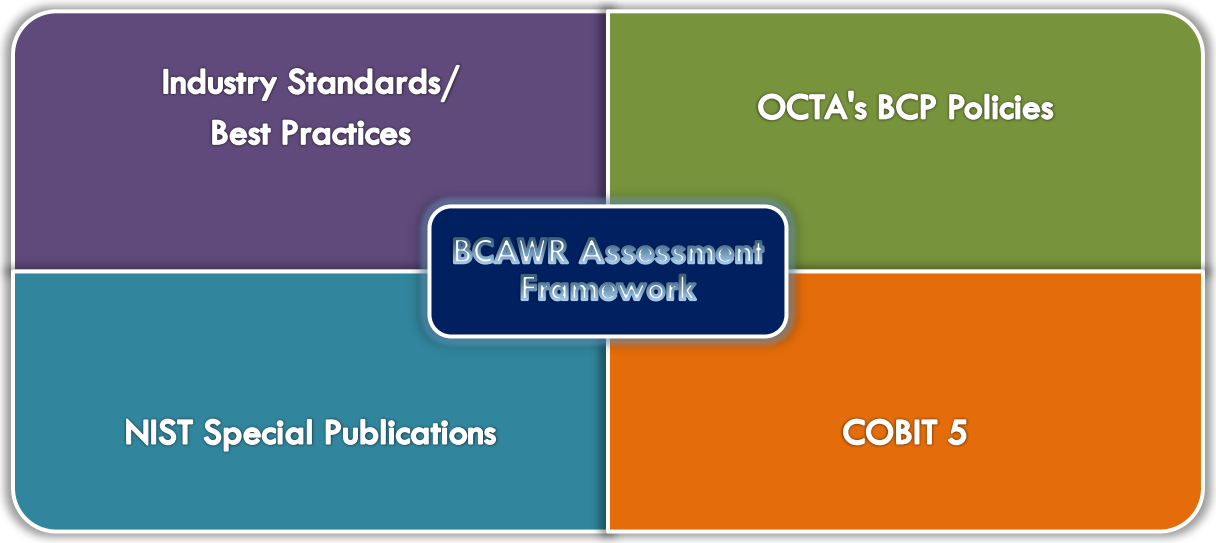
METHODOLOGY

This section contains the methodology used to assess the Plan based on the scope and objectives of this audit:

AUDIT STEPS	TESTING METHODOLOGY
Reviews and Observations	We requested and reviewed all relevant and existing Plan documentation including the Business Impact Analysis (BIA) performed by OCTA. We observed, where possible, activities related to the Plan maintenance and overall management process.
Inquiries and Meetings	We made inquiries of management and corroborated responses with appropriate operations personnel. We also conducted inquiries of personnel responsible for carrying out distinct aspects of the Plan and corroborated responses with other personnel and documentation. Our inquiries included interviews and meetings with key stakeholders of the Plan.
Examinations and Walk-Throughs	We inspected Plan documents and other related documentation to determine the adequacy and appropriateness of OCTA's Plan. We also determined whether the Plan development process was conducted in accordance with specific control policies and procedures, and any established industry standards. Our examination process involved reviewing and analyzing the Plan and related documents.
Substantive Testing	Extensive substantive testing was not necessary due to the current state of OCTA's Plan.

CRITERIA

To guide our audit and to adequately assess OCTA's Plan, our criterion was based on the requirements outlined in the agreement between OCTA and BCAWR, OCTA's policies, industry best practices, the Control Objectives for Information and related Technology (COBIT) 5, and the National Institute of Standards and Technology (NIST) Special Publications (SP). BCAWR used these criteria as the framework for the development of our audit methodology, findings, and recommendations. The audit was conducted in accordance with Generally Accepted Government Auditing Standards. Below is a pictorial representation of the criteria used.



SUMMARY OF FINDINGS

Based on the audit, we have concluded that:

1. **The BIA was not adequately and completely performed.**
2. **The Plan is not adequate.**
3. **Identified Alternate Facility Sites do not conform to best practices.**

These findings are discussed in more detail in the Detailed Audit Results section of this report along with our overall recommendation and management responses.

The remainder of this page is intentionally left blank.

INTRODUCTION AND BACKGROUND

On April 30, 2014 OCTA contracted with BCA Watson Rice to conduct a performance audit of OCTA's Plan.

OCTA is currently organized into eight divisions, as follows:

1. Chief Executive Office;
2. Capital Programs;
3. External Affairs;
4. Finance and Administration;
5. Government Relations;
6. Human Resources and Organization Development;
7. Planning; and
8. Transit.

OCTA obtained a grant to develop an entity-wide Plan and contracted with a consultant to develop the Plan. The consultant delivered the current Plan in May 2013 and this was the version delivered to BCAWR for the purpose of this performance audit. The Security and Emergency Preparedness office within the Transit division has primary responsibility for the development of the Plan.

The remainder of this page is intentionally left blank.

DETAILED AUDIT RESULTS AND MANAGEMENT'S RESPONSE

Finding No. 1: The BIA was not adequately or completely performed.

Condition – A BIA identifies, quantifies, and qualifies the impacts of a loss or interruption of services and activities, and provides information critical to the timing and prioritization of continuity and resumption strategies. A robust and thoroughly developed BIA is critical to the development of an effective Continuity Plan (Plan).

The BIA performed and documented for OCTA did not sufficiently address all critical functions and did not include information necessary for the development of an adequate Plan. For example, the BIA did not adequately address the following:

- Prioritization of critical business processes.

  While he BIA did identify 130+ "essential" functions, it lacks analysis that ranks these functions so that resumption can be adequately prioritized.

- Systems applications necessary for the resumption of critical activities and the related Maximum Tolerable Downtime[1].

  The Information Technology (IT) Department maintains a "Run Book[2]" that outlines 12 systems applications that must be brought up in the event of a disaster. The IT Department contracts with a backup site and performs testing to ensure that these 12 applications can be brought up. The systems identified in the "Run Book" were identified over two years before the BIA was performed. The current BIA did not review the "Run Book" applications in conjunction with the activities identified as critical to ensure that the systems identified are those that support essential activities. In addition, the BIA did not evaluate the maximum time OCTA can tolerate particular systems being down.

  As outlined in OCTA's Business Continuity Security Policy, the BIA should drive the development of the "Run Book"; it should address critical applications and their Recovery Point Objectives (the age of the files that must be recovered from back up storage for normal operations to resume), along with their order of precedent.

- Disruption scenarios and their relative likelihood and impact.

  The BIA does not specifically address any disruption scenarios. At a minimum, scenarios such as earthquake, fire, terrorism, or even a loss of commercial electric power should be addressed. Also, the likelihood of these disruptions has not been established. Along with these deficiencies, the impact of different disasters on specific functions of OCTA was not addressed.

[1] The maximum possible time OCTA can tolerate the system being down.
[2] Instructions for bringing up applications after a disruption or disaster.

The inadequacies of the BIA negatively impacted the development of the BCP. While OCTA has established a Business Continuity Security Policy, the BIA was not developed in accordance with this Policy, or with other established industry standards.

Criteria – *OCTA's Business Continuity Security Policy defines Critical Business Process as the processes identified within a BIA that are absolutely required for the creation or delivery of products or services. The policy further states that:*

1. *The BIA shall identify all OCTA Critical Business Processes;*
2. *The BIA shall provide a relative scoring for each Critical Business Process in order to establish prioritization;*
3. *The BIA for OCTA shall identify the tolerable downtime for each Critical Business Process; and*
4. *Downtime for each critical business process shall be measured in both Recovery Time Objectives (RTO) and Recovery Point Objective (RPO).*

Criteria - *NIST 800-53 RA-3 a. The organization conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.*

Cause and Effect – The BIA was not developed in accordance with OCTA policy or applicable industry standards. As a result, the BIA was not adequately or completely performed.

Finding No. 2: The Plan is not adequate.

Condition – After performing a BIA, the Continuity Plan (Plan) can be developed. The Plan is a set of written procedures designed to allow the OCTA to continue to perform essential functions in the aftermath of a disaster or disruption. When properly developed, the Plan will ensure that the people in critical jobs are available and have the systems, equipment, and facilities they need to provide essential services. Once developed, the Plan should be tested and regularly updated.

In May 2012, a Request for Proposals was issued for a firm to conduct a Business Impact Analysis, develop a Continuity Plan (Plan), and conduct training on the Plan. The COOP delivered by the consultant in May 2013 is inadequate and was not developed in compliance with OCTA policy or applicable industry standards, as follows:

- While the Plan identifies "essential functions", it lacks detailed procedures, equipment, and systems recovery plans to ensure that functions can be resumed. The Plan also lacks security measures to be taken during activation and operation of the Plan to ensure personally identifiable information (PII) and protected health information (PHI) are properly safeguarded.

- The contract with the consultant required training sessions be conducted on the Plan; however, this training occurred before the Plan was finalized. Interviews with employees that participated in the training and contributed to the Plan development stated that concerns as to the inadequacy of the

document were expressed during these sessions. Input, both verbal and written, and comments to the draft Plan were never addressed or incorporated into the final document.

- The Plan states that it "…has been adopted by the Board of Directors (Board)" and that "…the Chief Executive Officer has approved the Plan to ensure it is current and contains required information and guidance…" however, this is not the case.
- Appropriate security measures were not taken in the housing of the current version of the Plan. An electronic copy of the Plan is stored on a shared network drive; accessible to all employees and resident OCTA contractors. The Plan has sensitive information that should not be disclosed to employees and resident OCTA contractors that do not have a business need to know this information. This situation violates the "least privilege" principle.

- While the Plan identifies equipment that would be required in the event of a disaster, it lacks identification of a vendor from whom the equipment could be purchased in the event OCTA's equipment is not available for use.

- The Plan does not consider or interface fully with other OCTA plans, such as the Crisis Communications Plan and the Emergency Operations Plan, or consider coordinated plans with the County, State, or other agencies.

- Based on interview, Crisis Team members have not been provided adequate training related to their responsibilities in the event of an unscheduled interruption or disaster.

Criteria - *OCTA's Business Continuity Security Policy states that the BCP will be developed using guidance from the NIST 800 & 500 series documents. Best practices require that, in developing a comprehensive Business Continuity Plan, it is pertinent that a standard of best practices be selected by management to guide the process and to ensure that the plan is complete, thorough and effective. It also states that each BCP shall: "Implement appropriate security safeguards to ensure that OCTA's resources and sensitive information are secure".*

Criteria - NIST 800-53 states:

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates.

b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Criteria – *COBIT 5 is based on five principles. Principle #3 specifically relates to this situation. Principle #3, Applying a Single, Integrated Framework, states that a single integrated framework should be used for a Continuity Plan development and implementation.*

Criteria – *OCTA's Business Continuity Security Policy states that the BCP should address the following:*

1. *Processes or functions performed by an organization.*

2. *The resources required to support each process performed.*

3. *Interdependencies between processes (and/or departments).*
4. *The impact(s) of NOT performing each process.*
5. *The criticality of the process.*
6. *A Recovery Time Objective (RTO) for each process.*
7. *A Recovery Point Objective (RPO) for the data that supports each process.*

Criteria - *NIST 800-53 CP-1 Control Enhancement 1 The organization coordinates contingency plan development with organizational elements responsible for related plans.*

Cause and Effect- The Plan was not developed in accordance with OCTA policy or relevant industry standards. Management did not hold the contractor accountable to the deliverables required by the scope of work.

The developers of the Plan did not coordinate closely with the IT department. OCTA's Business Continuity Security Policy was developed and implemented by the IT department within the Finance and Administration Division. The Plan was developed and implemented by the Security and Emergency Preparedness Department within the Transit Division. As a result, detailed elements of OCTA's Business Continuity Security Policy were not addressed in the BCP. The final effect is a Plan that is noncompliant with OCTA's Business Continuity Security Policy.

The Plan has not been formalized due to the fact that those who commissioned the plan do not believe that the plan is ready to be formalized. However, the Plan was made available for distribution.

Without being formalized, there is no authority to implement any aspects of the Plan or hold any personnel responsible for any part of the Plan. Formal training and maintenance of the Plan cannot begin until the Plan is authorized and approved.

Finding No. 3: The BCP Alternate Facility Site does not conform to best practices.

Condition – An important element of a Plan is the identification of alternate facility sites for divisions needing to relocate in the aftermath of an event. The Plan in place includes an inventory of available facilities but the template has not been completed to reflect all of the site capabilities (e.g. available phone jacks and available data jacks). As such, it is not clear whether the sites selected by individual divisions as alternate facilities would meet their needs. Some of the administrative divisions / departments selected the building next door as an alternate facility while most others selected the Garden Grove location as their alternate facility. Whether that facility could accommodate all of these divisions / departments is also not addressed. Finally, the primary alternate facility does not meet the industry standard of being far enough from OCTA's main facility. Continuity experts advise organizations to select an alternate facility that has a 50 mile radius from the main facility so that it is not on the same commercial electrical grid and not subject to the same disaster scenario as would be the case if they are close together. Individual locations of the same organization within the same cluster can only provide limited alternate facility site coverage due to close proximity.

Criteria - *OCTA Business Continuity Security Policy:*

Each BCP shall:

- *Identify all required off-site computing, telecommunications systems, or storage locations necessary for operations restoration.*
- *Include detailed procedures for operation restoration.*

Criteria - *NIST 800-53 CP-7 Control Enhancement (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.*

Cause and Effect – The Plan does not include details of the capabilities of alternate facilities. The Plan does not reconcile the needs of divisions with the capabilities available at the alternate sites. The Plan does not determine whether the selected alternate sites can serve all of the divisions that plan to use it. In developing the Plan, management did not consider the common risks that exist between facilities. This could lead to an inability to perform continuity operations in the event of an incident.

Overall Recommendation:

We recommend that OCTA update the BIA in accordance with the existing Business Continuity Security Policy and then update the Plan accordingly to address all of the findings detailed in this report. The Plan development for an organization the size and complexity of OCTA is a significant project and it should be planned and executed utilizing industry standard best practices. We further recommend that OCTA consider performing an Independent Verification and Validation (IV&V) for the Plan development project.

An IV&V can provide the following benefits to OCTA:

- Independently hold the contractor accountable to the contract and scope of work for the BIA and Plan;
- Provide an independent and objective evaluation of deliverables prior to acceptance by OCTA; and
- Significantly contribute to OCTA's compliance with best practices and provide OCTA's key stakeholders with specific and relevant expertise to assist them in overseeing the BIA/Plan process.

Management's Response:

Staff welcomes the comments made by BCA Watson Rice (BCAWR) in their performance audit of OCTA's Continuity Plan and concurs with the assertion that the current Continuity of Operations Plan (COOP) and Business Impact Analysis (BIA) require additional work. However, it is important to note that the project was developed using a different set of industry standards than was used by BCAWR in their review.

BCAWR conducted their performance audit in accordance with Generally Accepted Government Auditing Standards and cited industry standards such as Control Objectives for Information and Related Technology (COBIT 5) and National Institute of Standards and Technology (NIST) 500 and 800. According to the consultant that prepared the plan for OCTA, the BIA was in fact developed consistent with a different set of professional practice standards, the Disaster Recovery Institute and the Business Continuity Institute, two recognized certification organizations in the Business Continuity Planning industry.

Also, OCTA's Business Continuity Security Policy was not used in the development of the BIA. In reviewing the two different standards, the performance audit exposed an area requiring much better integration and alignment. Future updates of the BIA and COOP will conform with applicable requirements of OCTA's Business Continuity Security Policy to better address technology requirements. As BCAWR stated in the Executive Summary, the current plans include some useful information for business resumption. While documents of this nature are constantly evolving due to changed circumstances, staff fully intends to build on the useful elements of the current plans and update them consistent with OCTA policy and appropriate industry best practices. After the existing plans were completed, staff began compiling material to update and refine the contents. Efforts have already commenced to update certain portions of the COOP and BIA, and as training and exercise activities are conducted throughout the year, it is likely that additional portions of each plan will be identified for modification during the lessons learned/after action report debriefing. Updates will be incorporated to the COOP and BIA within six months.

In an effort to accelerate a more comprehensive update, on September 4, 2014, staff secured $300,000 in Transit Security Grant Program funds from the Department of Homeland Security to complete a Threat and Hazard Identification and Risk Assessment (THIRA) project. The THIRA will help to identify specific disruption scenarios, their relative likelihood and impact on OCTA's operations. The THIRA will also include an update to the BIA to assist in OCTA's disaster recovery planning efforts. The entire effort is expected to take approximately 24 months to complete. Staff will also consider performing an Independent Verification and Validation (IV&V) of OCTA's Continuity Plan after researching the cost and benefits that an IV&V provides. In the interim, staff will continue to work toward updating sections of the COOP and BIA and work toward publishing revised editions of the plans on an annual basis.

Finally, while the audit specifically reviewed the COOP, it's important to acknowledge this is one piece of OCTA's overall emergency preparedness and response efforts. The COOP is essential in ensuring OCTA business can resume in the days and weeks following a disaster and does not reflect OCTA's ability to respond in a disaster or emergency situation. A separate document, OCTA's Emergency Operations Plan (EOP) is the primary document used in the event of a disaster and during the immediate aftermath of an incident. This plan contains the policies and procedures that direct the agency and operations given an incident of any nature. The EOP is regularly updated and OCTA has an active emergency management training and exercise program. OCTA plans and trains regularly with local, state and federal agencies involved in responding to disasters.