CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti
Risk & Business Consulting.
Internal Audit.

Executive Summary of the 2017 Business Continuity Management Review

Central Florida Expressway Authority

May 2017

Table of Contents

I. Executive Summary

Background

During the period between October 3 and November 4, 2016, Internal Audit ("IA") performed a Business Continuity Management ("BCM") review for the Central Florida Expressway Authority ("CFX"). The review focused on plans and procedures that CFX has in place to minimize the impact of interruptions to the business, such as: man-made, natural, and technological disruptions to either the geographic region or the corporate headquarters. BCM encompasses the development of strategies, plans, and actions which provide protection or alternative modes of operation for business processes in the event of the aforementioned interruption scenarios that could affect the organization.

Scope and Approach

The focus of this review included three (3) primary components. First, IA reviewed any current BCM, Crisis Management, or Disaster Recovery ("DR") documentation that was available, and second, determined whether the IT DR plan accounted for all components of CFX's IT infrastructure. Lastly, IA inquired with Management to determine the testing and training strategies in place to educate employees on the aforementioned plans.

To accomplish these objectives, Internal Audit:

- Evaluated the structure of the Agency's Crisis Management team and plan.
- Determined whether BCPs and the recovery strategies were founded on the Business Impact Analysis ("BIA") exercise that was performed by IA in 2014 or other risk assessment activities which prioritize recovery efforts of the business and IT resources.
- Established an inventory of all critical departments and applications / systems at CFX and reviewed the departmental BRPs and IT DR strategies. For each document obtained, evaluated if:
    - The document included guidelines on response team roles and responsibilities.
    - The BRP/ DRP included guidelines on when the plan should be invoked and defined the members of the response teams.
    - Alternate work locations or IT recovery sites were established and could feasibly be utilized to operate in disaster scenarios.
    - The document included guidelines for external communication, including procedures that will be taken to re-establish communications with key third-party partners and notification procedures to customers or other stakeholders.
    - Management had taken into consideration short and long-term recovery scenarios, as well as guidance on how to restore the environment back to "normalcy" following the conclusion of a disaster event.
- Reviewed and evaluated the BRP and IT DR testing strategy, including the frequency and nature of testing, the use of alternate recovery sites for testing exercises, etc.
- Evaluated the training exercises that are conducted.
- Reviewed the strategies established from an IT DR perspective to mitigate the risks associated with malicious attacks to the IT environment (i.e. malware, virus, ransomware, etc.).

In order to accomplish this review, Internal Audit:

- Interviewed key personnel (i.e. CFX Security Manager, Corporate Department Leads, etc.)
- Performed a Risk Analysis of corporate departments at CFX to determine which would be included in the sample
- Reviewed documentation associated with the BCM, IT DR planning, and Crisis Management
- Performed walkthroughs of the recently completed Hiawassee data center

Summary of Findings

As a result of this review, Internal Audit identified five (5) observations that should be addressed in order to strengthen the overall BCM program at CFX. These observations refer to Business Continuity specific documents, plans, and training regimens that organizations typically have in place to plan for and assist in recovery efforts. The observations are grouped into the following three (3) high-level topics:

- IT Disaster Recovery
- Crisis Management Documentation and Training
- Business Continuity Management Documentation and Training

Recommendations

As a result of the observations made during the review, recommendations surrounding the following areas were developed:

- Connectivity to IT Backup Environment
- Crisis Management Documentation and Testing
- Business Resumption Plans and Training