OIO

Office of Integrity & Oversight

Government of the District of Columbia, Office of the Chief Financial Officer

August 26, 2020

PROACTIVE SURVEY REPORT OF THE OFFICE OF THE CHIEF INFORMATION OFFICER'S (CIO) COMPLIANCE WITH PROCEDURES RELATED TO DISASTER RECOVERY AND BUSINESS CONTINUITY

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Chief Financial Officer

Office of Integrity and Oversight

TO: Alok Chadda, Chief Information Officer
Office of the Chief Information Officer

FROM: Timothy Barry, Executive Director *Timothy Barry*
Office of Integrity and Oversight

DATE: August 26, 2020

SUBJECT: Final Report: Proactive Survey of the Chief Information Officer's Compliance with Policies Related to Disaster Recovery and Business Continuity (OIO No. 20-01-07 OCIO)

This report summarizes the results of the Proactive Survey of the Office of the Chief Information Officer (OCIO)'s Compliance with Policies Related to Disaster Recovery and Business Continuity. The proactive survey was designed to identify management issues and internal control deficiencies that may require immediate management corrective actions. The objective of this survey was to assess OCIO's compliance with the Disaster Recovery and Business Continuity Plan.

OIO provided one (1) recommendation to the Chief Information Officer, OCIO, for actions necessary to correct the described deficiencies. The OCIO provided a written response to the draft report on August 17, 2020. The OCIO agreed with the recommendation that a formal working group comprised of key stakeholders from across the OCFO needs to be formed to identify business processes and dependencies, define recovery timelines, and create a step-by-step incident response process, but disagreed that this working group be established and managed/led by the OCIO. The alternative proposed actions meet the intent of our recommendation. A copy of the response, in its entirety, is included as an Appendix to this report.

We appreciate the assistance and cooperation that you and your staff provided to OIO during this audit. Should you have any questions, please contact me at (202) 442-6433; or Tisha Edwards, Director of Internal Audit, at (202) 442-6446.

cc: Jeff DeWitt, Chief Financial Officer, OCFO
Angell Jacobs, Deputy Chief Financial Officer and Chief of Staff, OCFO
Marshelle Richardson, Chief Risk Officer, OCRO
Jatin Shah, Chief Information Security Officer, OCIO

Background

The Office of the Chief Financial Officer (OCFO) Office of the Chief Information Officer (OCIO), Chief Information Security Officer (CISO) is responsible for managing the Disaster Recovery and Business Continuity Plans for the Office of the Chief Financial Officer (OCFO). These contingency plans are in place to provide guidance to an organization in the event of a major disaster or emergency event.

The National Institutes of Standards and Technology (NIST) issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002. NIST guidelines are directed to federal agencies; however, they are also used by state governments and private organizations in managing cost-effective programs to protect their information and information systems. Special Publication 800-34 *Contingency Planning Guide for Federal Information Systems,* provides instructions, recommendations, and considerations for federal information system contingency planning. The District is not required to follow the guidelines; however, NIST guidelines are considered industry best practices.

Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity and disaster recovery planning. Additionally, the guidelines recommend that organizations use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility.

Special Publication 800-34 defines Disaster Recovery Contingency planning *(DRP)* as interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods.

The OCIO is responsible for managing the DRP for the OCFO. The OCIO developed policies and procedures for managing the Disaster Recovery and Business Continuity Plans that are based on the NIST guidelines. The guidelines require that the following components be included in a Disaster Recovery Plan:

- Contingency Plan
- Contingency Plan Training
- Contingency Plan Testing
- Alternate Storage Site
- Alternate Processing Site
- Telecommunication Services
- Information System Backup
- Information Recovery and Reconstitution

The *Business Continuity planning (BCP)* applies to recovery of the mission/business operations and pertains to the ability to continue critical functions and processes during and after an emergency event. This plan is developed collaboratively with the business units and addresses the information systems as well as business processes. Key elements of a BCP includes:

- Identifying business processes and dependencies.
- Defining recovery timelines; and
- Creating step-by-step incident response.

Objective, Scope, and Methodology

The objective of the proactive survey was to assess OCIO's compliance with the Disaster Recovery and Business Continuity Plans; however, our assessment was limited to the Disaster Recovery Contingency Plan (DRP) as the Business Continuity Plan (BCP) has not been developed.

To accomplish our objective, we requested the OCIO provide the current Policies and Procedures for Disaster Recovery. We assessed the procedures to determine whether they were designed in compliance with the National Institute of Standards 800-34. We met and held discussions with the relevant OCIO officials. We also reviewed relevant documentation to support OCIO's implementation of the Procedures. Although we were not able to visit the back-up sites due to the current COVID-19 crisis we reviewed pictures of the backup location and the contracts with the Vendors.

This engagement was a Proactive Survey and was therefore not conducted in accordance with Generally Accepted Government Auditing Standards.

Observations

Our assessment of the OCFO Disaster Recovery and Business Continuity Plans determined: 1) a Business Continuity Plan (BCP) has not been developed, and 2) the Disaster Recovery Contingency Plan (DRP) has not been fully implemented. Since there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. The lack of a BCP and fully implemented DRP, leaves the OCFO's emergency management at risk in the event of a major disaster.

A Business Continuity Plan (BCP) has not been developed.

During the entrance conference with OCIO officials we were informed that the OCFO does not have a BCP in place. Business Continuity and Disaster Recovery Plans are critical components of emergency management and organizational resilience. The Chief Information Security Officer (CISO), OCIO is aware that this plan is critical.

During FY 2019, the OCIO was involved in informal preliminary discussions regarding the development of a BCP internally and with OCFO business units. Additionally, a meeting was held with officials from the Office of Management and Administration and the OCFO Office of the Chief Risk Officer to discuss the development of a comprehensive emergency plan that includes a BCP and a Continuity of Operations Plan (COOP). Although these meetings were held, a formal plan or approach to developing the BCP, was not put in place.

In response to our questions, the CISO developed and provided OIO with a briefing document outlining the steps that need to be taken to develop a BCP (Appendix 1). In the document, the OCIO included placeholders for discussions on the recovery time expectations.

Based on the steps to be taken by the OCIO and the relevant parties, OCIO officials conclude that until the steps cited in the briefing document are discussed, agreed-upon and completed by the business units and other parties concerned, the BCP cannot be completed.

The OCFO Disaster Recovery Contingency Plan has been developed but is not Fully Implemented.

The OCFO Policies and Procedures for Disaster Recovery Contingency Plan (DRP) have been developed and comply with NIST 800-34 guidelines. However, we noted that some of the key components were not implemented or partially implemented. The following table shows the status of implementation:

Components	Status of Implementation
Contingency Plan	*Implemented.* The Contingency Plan Procedures were completed in March 2019.
Contingency Plan Training	*Not Implemented.* Training plans have not been developed.
Contingency Plan Testing	*Not Implemented*. The required annual testing has not commenced.
Alternate Storage Site	*Implemented.* The OCIO has a contract in place with a backup vendor. OIO could not visit the site due to Covid-19 restrictions; however, we reviewed the contract and pictures of the site configuration and the site appears to meet guidelines.
Telecommunication Services	*Partially Implemented*. The OCIO has designated a Telecommunication Service for the current Information Technology (IT) services; however, this will need to be updated when a BCP is developed.
Information System Backup	*Partially Implemented.* The OCIO has an Information System Backup, but it will need to be updated when a BCP is developed.
Information Recovery and Reconstitution	*Partially Implemented*. The OCIO has an Information Recovery plan for current IT systems, but it will be fully implemented when a BCP is developed.

Source: OIO

As noted above, training and testing have not been implemented. Additionally, responsibilities have not been assigned to the relevant Information Technology staff. The CISO, OCIO stated that the full implementation of the DRP requires the development of a comprehensive list of all systems and software that can be affected by a loss due to a disaster or other interruptions. This cannot be done without a BCP. The DRP should have been developed collaboratively with relevant business units to ensure that all components were fully addressed.

Recommendation:

We recommend the Chief Information Officer:

1. Establish a formal working group comprised of the OCIO personnel and key stakeholders within the OCFO business units to develop a BCP[1] that:

    - Identifies business processes and dependencies.
    - Defines recovery timelines; and
    - Creates a step-by-step incident response

[1] See Exhibit 1.

MANAGEMENT RESPONSE AND OIO EVALUATON

Management Response:

The OCIO agrees with the recommendation that a formal working group comprised of key stakeholders from across the OCFO needs to be formed to identify business processes and dependencies, define recovery timelines, and create a step-by-step incident response process, but disagrees that this working group be established and managed/led by the OCIO. Instead, the CIO believes this effort should be led by a non-IT senior executive of the business units, with the assistance of an external firm versed in this type of work.

OIO Evaluation of OCIO Response:

We recognize that the OCIO is not the only key stakeholders in the working group and should include leaders within the business unit. Based on further discussion with OCFO senior officials, the OCIO will work collaboratively with the Office of the Chief Risk Officer to solicit an experienced firm to assist in the development of the business continuity and disaster recovery plans for the OCFO. The proposed actions meet the intent of our recommendation and once implemented should resolve the deficiency identified.

APPENDIX 1 MANAGEMENT RESPONSE

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Chief Financial Officer

Alok Chadda
Chief Information Officer

Office of Chief Information Officer

MEMORANDUM

TO: Timothy Barry
Executive Director, Office of Integrity & Oversight

FROM: Alok Chadda, CIO
Chief Information Officer

DATE: August 17, 2020

SUBJECT: Draft Report: Proactive Survey Report of The Office of The Chief Information Officer's (CIO) Compliance with Procedures related to Disaster Recovery and Business Continuity (OIO No. 20-01-07 OCIO)

Thank you for providing us the opportunity to respond to your summary of the OCFO's compliance with policies regarding disaster recovery and business continuity. We agree with your assessment that the OCFO has not fully implemented its disaster recovery contingency plan nor has it developed a business continuity plan, and that this condition leaves the OCFO's emergency management capabilities at risk in the event of a major disaster. We also agree with your recommendation that a formal working group comprised of key stakeholders from across the OCFO needs to formed to identify business processes and dependencies, define recovery timelines, and create a step-by-step incident response process. Doing so will significantly strengthen the OCFO's ability to respond to a variety of scenarios such as a natural disaster, civil unrest, or a cybersecurity attack.

However, we do not agree with the portion of your recommendation that this working group be established and managed/led by the OCIO. The development of a business continuity plan is not an IT activity in which business units participate but rather the reverse: it is an essential aspect of business and risk management in which the IT organization participates. Of the three areas outlined in the table on page eight of the report we can take the lead on performing the next steps for further developing the OCFO IT Disaster Recovery Plan and for ensuring that each major system has an adequately documented and tested contingency plan. The development of business continuity plans for each business unit, the development of a crisis management plan, and the overall management of the effort, though, should be led by a senior executive from a non-IT office or business unit. We believe that that individual will be more effectively placed to function as the overall sponsor and champion of this effort and will be in a better position to ensure that the individual business continuity plans are meaningful and relevant. We acknowledge that we have limited in-house talent available to support the sponsor of this effort and that the services of a consulting firm will likely need to be engaged, but there are many firms in the area which are experienced in assisting governmental agencies do exactly this sort of work.

SW Waterfront, 1101 4th Street, SW, Suite W350, Washington, DC 20024
(202) 741-8700 Fax: (202) 442-6373

OCFO
Business Continuity Plan (BCP) Briefing

OCIO – May 2020

The BCP Conversation:

- If business continuity (BC) processes were invoked today for an issue, it would take at least (TBD) days to recover all Tier 1 processes for critical Business Unit. Total time to recover all OCFO critical business activities functions will be at least (TBD) days.
- Issues can vary from :
  - Environmental (Power , Fire , Earthquake , Water etc.)
  - Personnel , Pandemic , Terrorism(Union , COVID19 , Radioactive etc.)
  - Cybersecurity (Ransomware , Data Corruption , Software ,etc.)
  - Supply Chain (Vendor , Personnel , Cloud etc.)

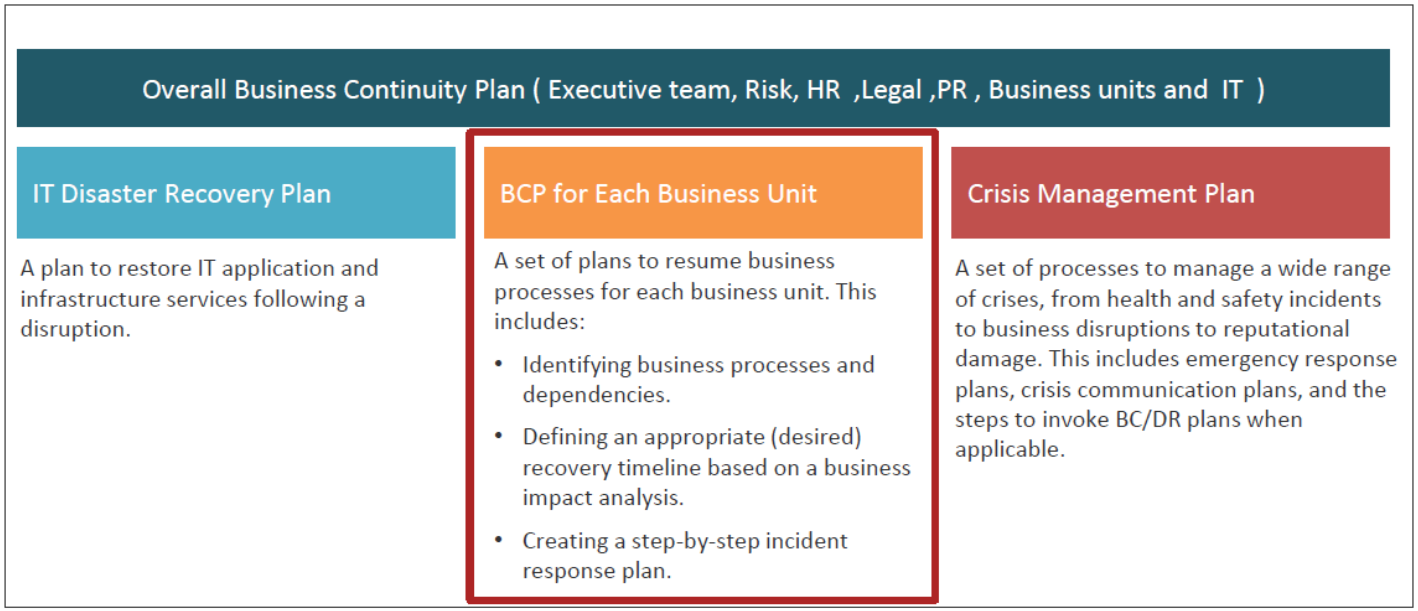
2

Why and Who ?

- Business Continuity Planning (BCP) is not a nice-to-have, it is a must-have.
- Business Continuity Planning (BCP) must be discussion in the Board Room / senior executives. It cannot reside inside a single department in Organization .

BCP ?

An overall Business Continuity Plan (BCP) is a holistic plan that includes IT Disaster Recovery Plan (DRP), a BCP for each business unit, and the crisis management plan



4

What We Can Do:

- BCP discussion at highest level in OCFO.
- BCP part of the organizational DNA
- Business process flowcharts (used to identify dependencies)
- Business impact analysis:
  - Scoring criteria (for critical business processes from different business units).
  - Impact scores
  - Tier 1, 2, and 3 criteria.
- Incident response plan
  - The event detection, notification, and escalation steps for all business units.
  - Identify gaps and risks to business units.
- BCP documenting and training (Workshop , Tabletop exercises)
- Keep BCP UpToDate.

5

What are the next steps:

- Start Business Continuity Planning (BCP) discussion in OCFO
- Identify business leaders responsible for Business Continuity Planning (BCP)
- Time and resource commitment for Business Continuity Planning (BCP)
- Focus on implementing a structured and repeatable process that can be applied to business unit one at a time to avoid BCP from becoming an overwhelming project.
- Enable business unit leaders to own the BCP by establishing a template that the rest of the organization can follow.
- Leverage BCP outcomes to refine IT Disaster Recovery (DR) objectives and achieve business alignment.
- Perform Table top exercise to simulate the Business Continuity Planning scenarios
- Perform Dry Runs/Fire Drills yearly to validate the plans
- Reduce overall risk to OCFO organization

OCFO BCP Briefing

Questions / Comments

OCFO BCP Briefing

Thank you!!!

8