Baruch COLLEGE

Alumni and Donor Giving (ADG): Data Backup & IT DRP

December 2022

Internal Audit and Services

Table Of Contents:

Objective:

The objective of this review is to assess the **Data Backup & IT DRP** process for the Alumni and Donor System (ADG).

Scope:

The scope included the following areas:

- Obtain an understanding of the data backup and IT DRP
- Verify Data backup is configured
- Verify that data backup is being monitored
- Verify that Data backup has encryption
- Verify that IT Disaster Recovery Plan is in place
- Verify that there's a business Impact Analysis
- Verify that IT DRP testing is enabled
- Verify that there is training personnel

Distribution and Audit Team

Distribution	Audit Team
Michael Goodman	Malik, Iqra
- Murat Pierre	Rasheda, Maham
	Cuadros, Genesis

Detailed Observations, Recommendations and Management Responses

#	Observation and Risk - Data Backup and IT DRP	Priority	Recommendation	Management Responses
1.	**Observation Summary:** The Bearcat system does not comply with the CUNY IT Data Backup policies. **Detailed Observations:** We noted the following: **SASLINUX** was confirmed to be updated daily, with a total of 8 backups a. 3 were unsuccessful b. 4 were successful c. The server didn't execute a backup on April 7th **LANGRP** performed daily backups, totaling 7 a. 1 was unsuccessful b. 3 were successful c. 2 were incomplete, and 1 wasn't executed **Amazon Web Services (AWS)** performed monthly backups, totaling 7 a. 3 were successful b. 2 were incomplete c. 2 were not executed **All three servers was not encrypted** **Risk Statement:** A lack of successful backups can put confidential data at risk. If data loss occurs, there is no way to recover sensitive information about the organization. Lack of encryption increases the organization's chances of suffering from a cyber attack.	*H*	Coordinate with CUNY IT Office of Data Backup to continue to perform periodic system backups. Also, consider backing up AWS daily instead of monthly. Regulate Bearcat database and servers with proper encryption. Create processes for routinely reviewing backups, keeping an eye out for failures in critical data, and ensuring that failed jobs are promptly fixed.	Agreed. **Responsible Party:** Murat Pierre (Director, System Backup and Recovery)

#	Observation and Risk - Data Backup and IT DRP	Priority	Recommendation	Management Responses
2.	**Observation Summary:** The firm has no IT Disaster Recovery Plan in place, as there was no record of it in the evidence. **Detailed Observations:** We noted the following: 1. AWS consists of IT Disaster Recovery however, their system is not feasible to use 2. Failure in identifying which systems need to be received 3. The client fails to have proper training in place during a situation of disaster 4. The data back ups are not tested. **Risk Statement:** Failure to establish an IT Disaster Recovery Plan may result in critical data being in jeopardy.	*H*	Implement Bearcat to have an IT Disaster Recovery Plan in place. Require formal request, approval, and testing of all application changes and retain documentation. Implement proper training so staff will be able to perform backups better. Require that all backups be tested. Identify important data that must be recovered in case of a disaster.	Agreed. **Responsible Party:** Murat Pierre (Director, System Backup and Recovery)