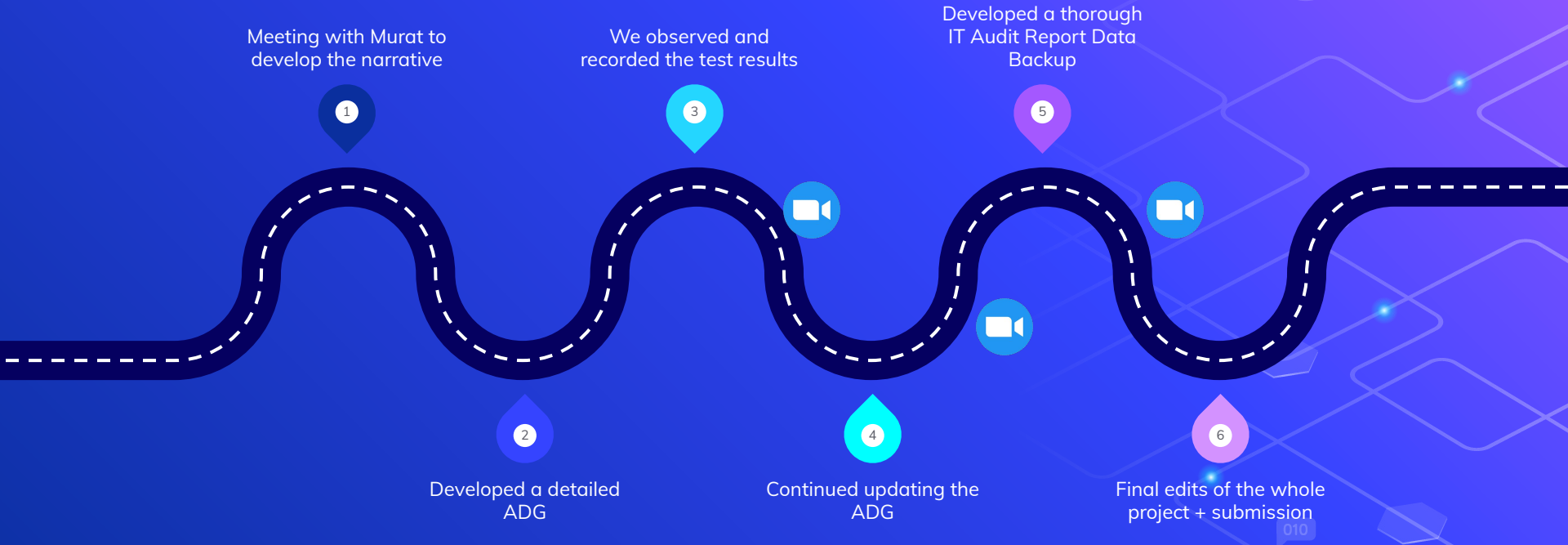
Data Backup & IT Disaster Recovery Plan (DRP)

CIS 4350 - Group 5

Roadmap


Meeting with Murat to develop the narrative
1
Developed a detailed ADG
2
We observed and recorded the test results
3
Continued updating the ADG
4
Developed a thorough IT Audit Report Data Backup
5
Final edits of the whole project + submission
6

Audit Team

Maham Rasheda

Iqra Malik

Genesis Cuadros


Michael Goodman
IT Vice President, Alumni/Donor Giving
Melissa Belvant
Senior Director, Identity & Access Mgmt.
Jean Similien
Senior Director, Infrastructure Operations
Virgilie Fannon
Senior Director, Interfaces and Integrations
Melinda Miller
Director, Change & Configuration Mgmt.
Murat Pierre
Director, System Backup & Recovery

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

Narrative

Notes from Murat Pierre

Data Backup Configuration

- Oracle Data Integrator
- They are either backed up on a weekly or monthly basis, depending on the server being used.

Data Backup Monitoring

- Tivoli, an IBM tool to back-up data.
- User receives a warning messages alerts, and alarms via email = failure in backup
- User will continue to troubleshoot

Data Backup Encryption

- Data backups are not encrypted on premises
- Encrypted on AWS cloud in a non-readable format.
- Client uses TLS for encrypting data in transit and protecting data privacy.

IT Disaster Recovery Plan (DRP)

- The client mentioned that they have no plan in place, but AWS does
- There is a failure in identifying which systems need to be recovered.
- Client doesn't have proper training in place for staff. Data backups are not tested.

#	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 **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: a. AWS consists of IT Disaster Recovery however, their system is not feasible to use b. Failure in identifying which systems need to be received c. The client fails to have proper training in place during a situation of disaster d. The data back ups are not tested. **Risk Statement:** Failure to establish an IT Disaster Recovery Plan may result in critical data to be 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)

THANK YOU!