BIENNIAL PERFORMANCE AUDIT OF THE BALTIMORE CITY INFORMATION AND TECHNOLOGY

JOSH PASCH, CPA

CITY AUDITOR

JULY 24, 2024 – PRESENTATION TO THE BOARD OF ESTIMATES



OUTLINE



1. Audit Objectives and Scope
2. Risks Identified For Review
3. Audit Methodology
4. Background Information
5. Findings
6. Implementation Status of Prior Findings
7. Questions?

AUDIT OBJECTIVES AND SCOPE

- Evaluate whether the recovery priorities (critical and important systems) set by the Baltimore City Information and Technology (BCIT) are consistent with the City of Baltimore's assessment or best practices
- BCIT has appropriate continuity and recoverability plans and infrastructure
- Follow-up on findings and recommendations that were included as part of the previous biennial performance audit report dated November 01, 2022
- Scope - Fiscal Years 2022 and 2021 and Information Technology Disaster Recovery Plan (ITDRP)



RISKS IDENTIFIED FOR REVIEW

- Operational risk
- Data Security risk
- Information Technology risk



AUDIT METHODOLOGY

- Identified and reviewed applicable standards, including documents published by the National Institute of Standards and Technology, and the State of Maryland
- Reviewed the draft ITDRP, including compliance with relevant standards
- Interviewed and / or inquired of key personnel of BCIT to obtain an understanding of the processes, procedures, and internal controls related to the disaster recovery
- Analyzed the key risks associated with creation of the Citywide list of critical applications, recovery processes, procedures and testing, and backup of City data

AUDIT METHODOLOGY (CONTINUED…)

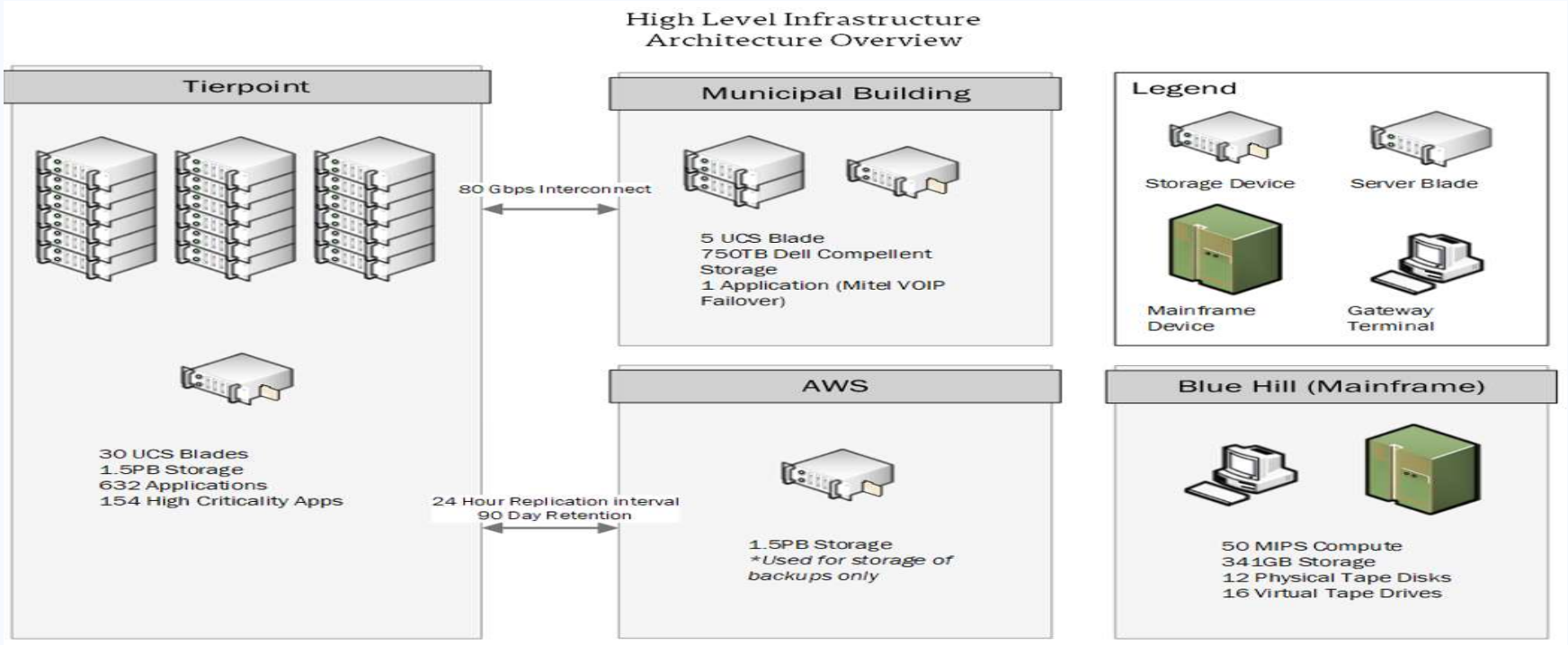
- Reviewed documentation of backups performed to determine whether the backups occurred as stated in the ITDRP and were complete
- Tested all nine quarterly restoration tests to determine whether they addressed the ITDRP testing requirements
- Reviewed contracts and Systems and Organization Controls Type II reports of vendors for City's backup sites

INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN

- When - March 2020
- By whom - Consultant and BCIT
- Applicable Standards – NIST and State of Maryland

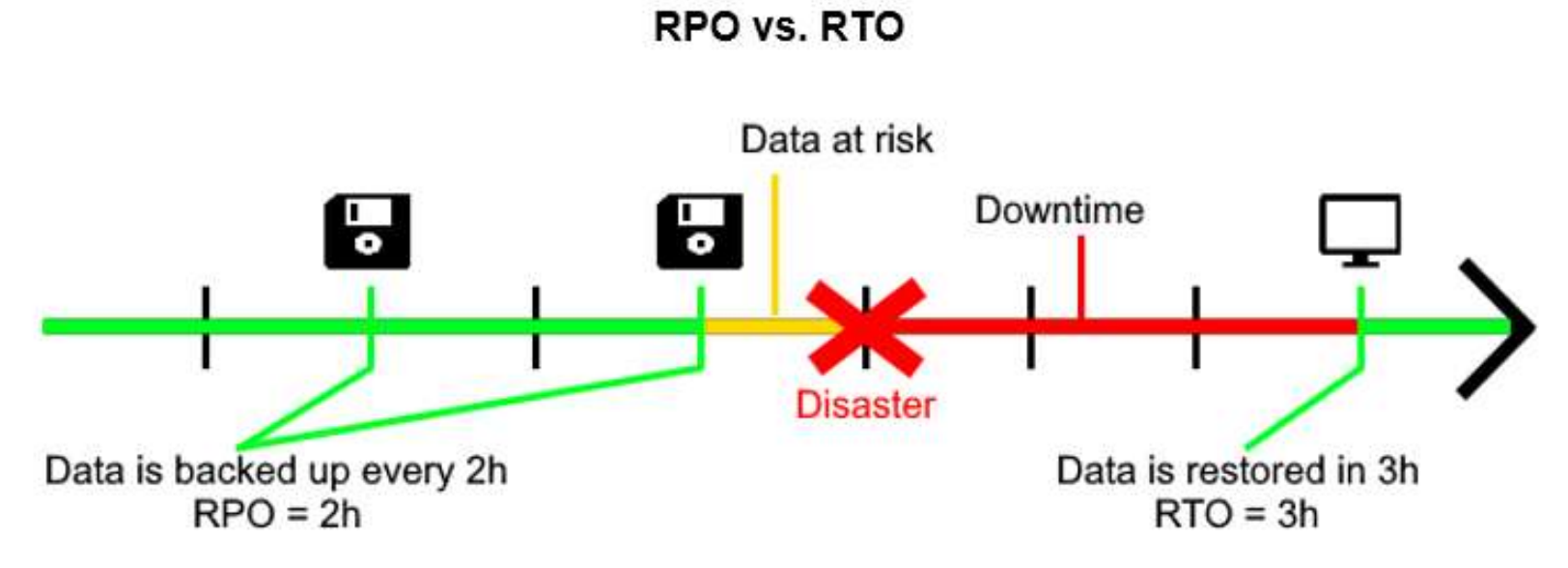
Note: The NIST is part of the U.S. Department of Commerce. It is the standard-setting agency that develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.

IT DRP PROCESS



Source: IT DRP

RECOVERY OBJECTIVES



Note: RPO = Recovery Point Objective; RTO = Recovery Time Objective

BUSINESS IMPACT ANALYSIS

- Identifies the priority for each application and includes the recovery expectations
- Helps agencies establish target recovery objectives such as RPO and RTO



CRITICAL APPLICATIONS AND SYSTEMS

Category	Definitions	DRP Exercises
0	Core Infrastructure (e.g., Core Network components, Active Directory, backup systems),	Annual
1	Applications that support mission critical services, such as public safety	Annual
2	All other applications and systems, with a priority focus on applications that support the finance function	Biannual

Source: IT DRP

BACKUPS

The BCIT:

- Automatically backs up the entire City's data daily, weekly, and monthly except for certain agencies that have backups performed by third-party vendors.
- Utilizes two backup sites (Blue Hill and TierPoint) and cloud storage services managed by third party service providers to provide robust capacity and quick response to disruptive events.

FINDING I

- **Caption** - The City does not have a fully documented disaster recovery plan that reflects the current hybrid (on and off premise applications and infrastructure) computing environment.

- **Condition** – The City:

  - Has invested in significant back up practices but has not fully invested in recovery practices.

  - Does not have a fully documented DRP, including Technical Recovery Procedures for use during an actual disaster recovery and the related exercises to return the City to normal operations.

FINDING I (CONTINUED...)

- **Effect** - A fully documented DRP including Technical Recovery Procedures facilitates the City in mitigating the impact of operational, financial, and service risks and supports the return-to-normal operations following a disaster.

- **Cause** - According to BCIT, limited staffing has impacted its ability to complete the DRP and formally document the related technical recovery procedures.

FINDING I (CONTINUED...)

Recommendation I - We recommend the Chief Information Officer (CIO):

- Re-evaluate, update, formalize, and implement the consultant's DRP recommendations to be reflective of current and future City computing environment;

- The plan should contain realistic DRP assumptions, appropriate technical recovery procedures and meet requirements of agency Continuity of Operations Plans (COOP).

FINDING II

- **Caption** - The City does not have a complete list of critical applications that is consistent with the disaster recovery plan and COOP expectations, including targeted recovery objectives for all critical applications.

- **Condition** - BCIT has not completed a Citywide Business Impact Analysis (BIA) and updated the DRP.
  - As of March 31, 2024, the impact analysis and determination of the criticality of applications with targeted recovery objectives has only been performed for four City agencies.
  - The complete applications list should include the agency owned and managed applications that are backed up by third party vendors.
    - The responsibility for DRP for these applications has not been defined.

FINDING II (CONTINUED...)

- **Effect**
  - The absence of the BIA may result in mis-prioritization or missed critical services.
  - Lack of oversight responsibility for agency applications that are restored by third parties may impact the ability of the respective agencies to return to normal operations in the event of a disaster.

FINDING II (CONTINUED…)

Recommendation II: We recommend the CIO:

- Conduct meetings with the respective City agencies and Mayoral offices to:
  - Revise and update key terminology and definitions of criticality, recovery time objectives, roles and responsibilities etc.;
  - Compile a complete list of critical applications across the City, including specific agency applications backed up by third party vendors, and determine criticality; and
  - Establish governance and oversight for DR, including roles and responsibilities for BCIT managed applications, as well where agencies' applications are backed up by third party vendors or if agency IT units are in place.
- Work with the Chief Administrative Officer, the Director of the Department of Finance (DOF), and Office of Emergency Management (OEM) to update Administrative Manual guidelines (e.g., AM-110-1 *Continuity of Operations Plan*) to incorporate requirements for agencies to develop BIA in coordination with BCIT.

FINDING III

- **Caption** – The BCIT does not have test plans to fully comply with the restoration testing requirements for all critical applications.

- **Condition**-

  - The BCIT has not developed test plans and schedules to fully comply with the DRP restoration testing requirements.

    - From March 11, 2022 through March 31, 2024, BCIT performed nine quarterly restoration tests across servers for three agencies (including BCIT).

    - The testing was limited and addressed Infrastructure applications (category 0) and three applications for three agencies (category 2).

    - The testing was not adequately documented and there was no evidence of completion for six of nine tests, or 67 percent.

  - Neither BCIT nor agency IT units have coordinated and validated test results for the restorations performed by vendors on behalf of the City.

FINDING III (CONTINUED…)

- **Effect -** The BCIT cannot demonstrate that the City's applications and operations can be successfully restored in the event of a disaster.

- **Recommendation III:** We recommend the CIO:

  - Develop a cost-effective coordinated test plan for all critical City applications. Based on the test plan, develop a reasonable schedule to perform restoration testing for Categories 0, 1, and 2, and resolve any issues identified during testing;

  - Coordinate and validate testing restorations performed by vendors or managed by agency IT units on behalf of the City; and

  - Retain documentation, including test plans and evidence of completion.

IMPLEMENTATION STATUS OF PRIOR FINDINGS

No.	Finding	Auditor's Assessment
1.	Controls are not established for Expenditure Authorizations, while the controls over P-card purchases are limited.	Implemented
2.	There is no comprehensive list of critical applications deployed across the City.	Partially Implemented

IMPLEMENTATION STATUS OF PRIOR FINDINGS (CONTINUED…)

No.	Finding	Auditor Assessment
3.	BCIT Infrastructure does not have formal policies and procedures for documentation of IT software procurement review process.	Implemented
4.	The City's Administrative Manual (AM) Sections for Computer Systems and Services are outdated and are not reflective of the current practices, thus creating ambiguity.	Not Implemented



Questions?