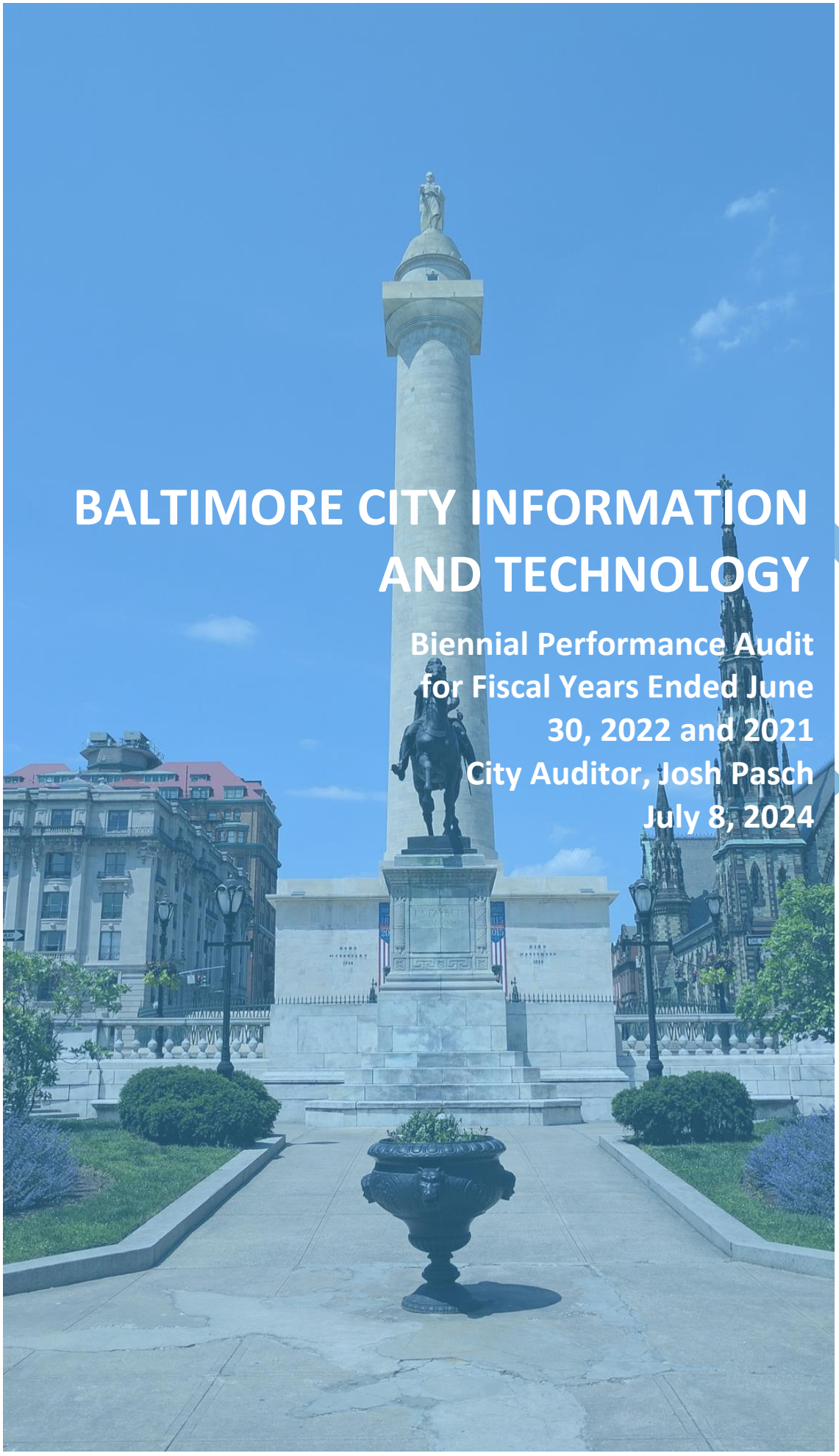


# BALTIMORE CITY INFORMATION AND TECHNOLOGY

## Biennial Performance Audit for Fiscal Years Ended June 30, 2022 and 2021

City Auditor, Josh Pasch

July 8, 2024

## CONTENTS

Office of the Comptroller
**Josh Pasch, City Auditor**
100 N. Holliday St., Room 321
Baltimore, Maryland 21202

Honorable Bill Henry, Comptroller
and Other Members
of the Board of Estimates
City of Baltimore

# Executive Summary

We conducted a *Biennial Performance Audit of Baltimore City Information Technology for the Fiscal Years Ended June 30, 2022 and June 30, 2021*. The objectives of our performance audit were to: (1) evaluate whether the recovery priorities (critical and important systems) set by Baltimore City Information and Technology (BCIT) are consistent with the City of Baltimore's assessment or best practices; (2) BCIT has appropriate continuity and recoverability plans and infrastructure; and (3) follow-up on findings and recommendations that were included as part of the previous performance audit report of BCIT, dated November 1, 2022. The scope of our audit is fiscal years (FYs) 2022 and 2021; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify information during the audit period.

The City's disaster recovery plan (DRP) was drafted by a consultant in March 2020. The consultant made multiple recommendations for the City of Baltimore (City) to continue improving the DRP. As of the time of our audit, those recommendations have not been fully implemented. Even though the DRP is still in the draft stage, BCIT is following it. However, the BCIT has the opportunity to strengthen the DRP. Specifically, the draft DRP does not include:

- Technical Recovery Procedures. The procedures should detail the processes and steps to recover the City's infrastructure and data from the various cloud-based storage vendors and Mainframe applications and systems. The procedures should also include end-user validation of the accuracy and completeness of the recovered data;

- Complete list of critical applications with targeted recovery objectives[1]. The BCIT current list includes specific applications from four agencies[2]. Also, the list does not include the agency owned and managed applications that are backed up by third party vendors[3]. However, the responsibility for DRP for these applications has not been defined (note: this is not applicable to cloud-based applications);

- Business impact analysis (BIA). The BIA identifies the priority for each application and includes the recovery expectations. The absence of the BIA may result in mis-prioritization or missed critical services; and

[1] The targeted recovery objectives include: 1) the recovery point objective (RPO), which is the time between the last backup and when the event occurs and will be the data available to be recovered; and 2) recovery time objective (RTO), which is how long it takes to recover data and resume operations.

[2] Four agencies are the Department of General Services (DGS), Department of Housing and Community Development (DHCS), Department of Law (DOL), and Department of Transportation.

[3] For example, the Baltimore City Health Department has a local area network and has a third party doing back up and restoration.

- Sufficient restoration testing program to determine whether BCIT can recover critical systems and data across City agencies and Mayoral offices. Currently, the BCIT performs periodic restoration testing for some agencies. Third-party vendors, such as Blue Hill[4], independently performs restoration testing; however, BCIT does not coordinate and validate test results for the restorations performed by vendors on behalf of the City.

Without a complete DRP that includes the items listed above and sufficient restoration testing, BCIT cannot demonstrate its ability to restore the City to normal operations in the event of a major disaster.

According to BCIT, limited staffing has impacted their ability to complete the DRP and formally document the related Technical Recovery Procedures.

Of the four prior audit recommendations that we followed up as part of this Biennial Performance Audit (See Section II on page 11), two recommendations, or 50 percent, were implemented, one recommendation, or 25 percent was partially implemented, and one recommendation, or 25 percent, was not implemented. The objective of prior audit was to evaluate whether the City has adequate policies and procedures to guide the Information Technology (IT) procurement processes to increase the efficiency and effectiveness of IT operations and costs.

To strengthen the DRP, we recommend the BCIT Chief Information Officer (CIO) implement the recommendations made in this report. Management responses are included in Appendix I (see page 17).

We wish to acknowledge the cooperation BCIT extended to us during our audit.

Respectfully,

Josh Pasch

Josh Pasch, CPA
City Auditor
Baltimore, Maryland
July 8, 2024

[4] Blue Hill is the backup vendor for the City's Mainframe applications. Blue Hill is contractually responsible for performing restorations on behalf of the City. As of March 2024, the Department of Audits has not received evidence of restoration testing performed by Blue Hill.

## Background Information

The Baltimore City Information Technology (BCIT) delivers a spectrum of technology services to both the City agencies and the community. These include traditional IT services, such as computer support, enterprise applications, and data networks, as well as a data service center and 3-1-1 Call Center.

The BCIT provides sustainable infrastructure and technology to support and enhance City departments, communities, and businesses to meet City and mayoral goals. Over the next decade, BCIT plans to engage all City agencies, businesses, and residents to design, build, and implement technology that creates a safe, thriving, and smart City. The City is deploying significant resources towards improving technology within the City. Given its strategic IT role, the BCIT is making determined changes to transform agencies and IT operations across the City government and the community.

**Key Terms**

- A disaster is an event that creates an inability to provide services for some determined period of time.[1]
- Disaster recovery is the ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's business functions.[1]
- DRP is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.[2]

**Sources:**

[1] State of Maryland Information Technology Disaster Recovery Guidelines Version 4.0 July 2006

[2] National Institute of Standard and Technology (NIST) Special Publication 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems May 2010.

The BCIT along with the agencies manage the infrastructure and applications to provide services to the residents. The BCIT is conscious of the vulnerability risks of its IT infrastructure, hardware, and applications to a disaster or a disruptive event and the need to put appropriate disaster recovery processes and capacity in place to enable the City to quickly recover its mission-critical functions and processes in the event of a disaster. Therefore, BCIT has developed a DRP to provide guidance for the management and recovery of critical infrastructure, processes, and services following a disaster, using current recovery capabilities. A DRP is a documented, structured approach that describes how an entity can quickly resume normal operations following an unforeseen event. It is a subset of a business continuity plan and revolves around the aspects of an organization that rely on a functioning IT infrastructure. The BCIT has developed the DRP in compliance with the relevant standards issued by the NIST [5] and the State of Maryland.

[5] 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.

As part of its disaster recovery capabilities, BCIT utilizes two backup sites and cloud storage services managed by third party service providers to provide a robust capacity and quick response to disruptive events. These backup sites and cloud storage services will recover data on behalf of the City to support the return to normal operations. Backups protect against human errors, hardware failure, virus attacks, power failure, and natural disasters.

## Significant Improvements Since March 2020 Noted by BCIT

According to BCIT, it has transformed the landscape of information technology in the City of Baltimore. This includes providing the infrastructure for employees to work offsite, whether at home or an alternate location, through Virtual Desktop Infrastructure (VDI). Furthermore, all data that is backed up in the on-premises data center has ransomware encryption protection enabled. This data is also backed up to a secondary location at one of our cloud service providers. As a result, the DRP needs to be updated to reflect current state; however, BCIT does not have adequate resources to ensure the DRP remains updated.

## Objectives, Scope, and Methodology

We conducted our performance audit in accordance with G*enerally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of our audit were to:

- Evaluate whether the recovery priorities (critical and important systems) set by BCIT are consistent with the City's assessment or best practices;
- Evaluate whether BCIT has appropriate continuity and recoverability plans and infrastructure; and
- Follow-up on prior findings and recommendations included in the previous Biennial Performance Audit Report, dated November 1, 2022.

The scope of our audit is FYs 2022 and 2021; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify the information during the audit period.

To accomplish our objectives, we:

- Identified and reviewed applicable standards that included documents published by the: (1) NIST; and (2) State of Maryland;
- Reviewed the draft DRP, including compliance with relevant standards;
- Interviewed and / or inquired of key personnel from BCIT to obtain an understanding of the processes, procedures, and internal controls related to the DRP;
- Analyzed the key risks associated with creation of the Citywide list of critical applications, recovery processes, procedures and testing, and backup of City data;
- Reviewed documentation of backups performed to determine whether they occurred daily as stated in the DRP and were complete;
- Tested all nine quarterly restoration tests to determine whether they addressed the DRP testing requirements; and
- Reviewed contracts and Service Organization Controls Type II reports of vendors associated with the City's backups and restoration activities.

# SECTION I: Current Findings and Recommendations

### Finding I: The City Does Not Have a Fully Documented Disaster Recovery Plan that Reflects the Current Hybrid Computing Environment[6].

The City has invested in significant back up practices but has not fully invested in the recovery practices. The City does not have a fully documented DRP including Technical Recovery Procedures[7] for use during an actual disaster recovery to return the City to normal operations. Currently, the City has a draft DRP dated March 27, 2020[8], which BCIT follows. According to BCIT, limited staffing has impacted their ability to complete the DRP and formally document the related Technical Recovery Procedures**.**

The NIST Special Publication 800-34 Rev. 1 *Contingency Planning Guide for Federal Information Systems* identifies a seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems. Of the seven steps, the following steps are relevant to this finding:

1. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

2. Ensure plan maintenance. The plan should be a living document updated regularly to remain current with system enhancements and organizational changes.

**Recommendation I:** We recommend the CIO re-evaluate, update, formalize, and implement consultant's DRP recommendations to be reflective of current and future City computing environment. This plan should contain realistic DRP assumptions, appropriate technical recovery procedures and meet requirements of agency Continuity of Operations Plans (COOP).

[6] Hybrid computing environment includes on and off premise applications and infrastructure.

[7] The procedures should detail the processes and steps to recover the City's infrastructure and data from the various cloud-based storage vendors and Mainframe applications and systems. The procedures should also include end-user validation of the accuracy and completeness of the recovered data.

[8] The DRP was developed by a consultant. The consultant included recommendations for the City to complete the DRP.

## Finding II: The City Does Not Have a Complete List of Critical Applications That Is Consistent with Disaster Recovery Plan and Continuity of Operations Plan Expectations, Including Targeted Recovery Objectives for All Critical Applications.

The draft DRP dated March 27, 2020 recommends conducting a Citywide BIA; however, BCIT has not completed the respective analysis and updated the DRP. As of March 31, 2024, the impact analysis and determination of the criticality of applications has only been performed for four City agencies[9]. For the four agencies, the City does have a list of critical applications with targeted recovery objectives.

Additionally, according to BCIT, the complete applications list should include the agency owned and managed applications that are backed up by third party vendors. For example, the Baltimore City Health Department has a local area network and has a third party doing back up and restoration. However, the responsibility for DRP for these applications has not been defined (note: this is not applicable to cloud-based applications).

The BIA identifies the priority for each application and includes the recovery expectations. Additionally, the BIA helps agencies establish target recovery objectives such as RPO and RTO. The absence of the BIA may result in mis-prioritization or missed critical services. Furthermore, the absence of assigned oversight responsibility for agency applications that are restored by third parties may impact the ability of the respective agencies to return to normal operations.

According to the City's DRP, "the City of Baltimore should conduct a business impact analysis annually to properly categorize applications and identify required resources during disaster situations." RPO and RTO are defined in the City DRP as follows:

- **Recovery Point Objective:** Point (measured in time) to which information used by an activity must be restored to enable the activity to operate on resumption. This can also be referred to as "maximum data loss."

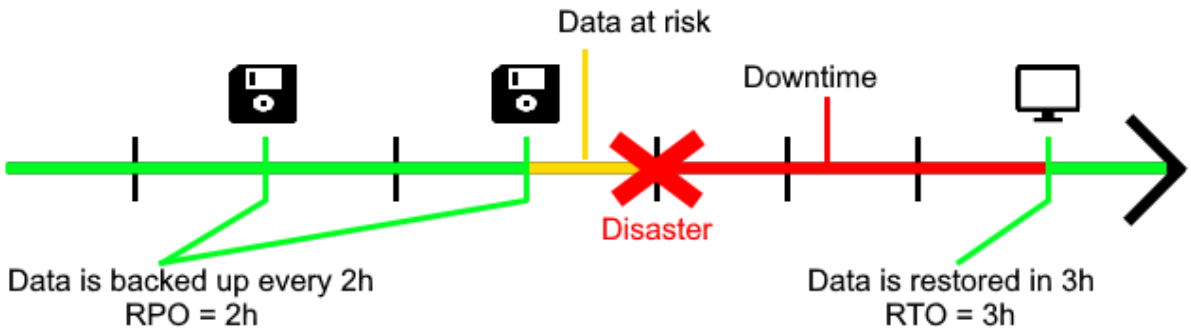
- **Recovery Time Objective:** Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.

The RPO is the time between the last backup and when the event occurs and will be the data available to be recovered, and RTO is how long it takes to recover data and resume operations.

[9] Four agencies are DGS, DHCD, DOL, and DOT.

**Illustration I**

**RPO vs. RTO**




According to the NIST Special Publication 800-34 Rev. 1 *Contingency Planning Guide for Federal Information Systems*, an agency should "Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission / business processes."

**Recommendation II:** We recommend the CIO conduct meetings with the respective City agencies and Mayoral offices to:

- As part of the development of DRP, 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 as, when agencies' applications are backed up by third party vendors or if agency IT units are in place.

We also recommend the CIO to work with the Chief Administrative Officer and the Director of 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 requirement for agencies to develop BIA in coordination with BCIT.

## Finding III: The BCIT Does Not Have Test Plans to Fully Comply with the Restoration Testing Requirements for All Critical Applications.

The BCIT is not in full compliance with the DRP restoration testing requirements included in the draft DRP dated March 27, 2020. As a result, BCIT cannot demonstrate that City applications and operations can be successfully restored in the case of a disaster.

**Critical Categories**

- Category 0 contains core infrastructure (e.g. core network components, Active Directory, and backup systems);
- Category 1 contains the applications that support mission critical services such as public safety; and
- Category 2 contains all other applications and systems, with a priority focus on applications that support the Finance function.

**Source:** City's DRP

**The Absence of Test Plans and Schedules for Citywide Restoration Testing:** The DRP states that restoration testing will be performed annually for Categories 0 and 1, and bi-annually for Category 2. 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 the following two of the three critical categories:

- Infrastructure applications (category 0); and
- Three applications for three agencies (category 2).

The testing was not adequately documented (e.g., test plans with expected outcomes), and there was no evidence of completion (e.g., a screenshot of target server with control totals, date and time, failed count, status (success or failure, etc.…) for six of nine tests, or 67 percent.

**No Coordination and Validation of Vendors' Restoration Test:** The BCIT nor agency IT units have coordinated and validated test results for the restorations performed by vendors on behalf of the City. For example, Blue Hill is the backup vendor for the City's Mainframe applications. Blue Hill is contractually responsible for performing restorations on behalf of the City. As of March 2024, the Department of Audits has not received evidence of restoration testing performed by Blue Hill.

According to the draft DRP, testing is "An evaluation tool that uses metrics to validate the operability of a system or system component in a production environment specified by the DRP. A test plan can be developed to identify metrics and systems for testing. Examples of tests include:

- Testing the execution and effectiveness of disaster-condition communications procedures within a prescribed time limit;

- Removing power from a system or component;

- Execution of a failover procedure to an alternate data center within a certain timeframe; and

- Conducting infrastructure component and application recovery test in a User Acceptance Testing environment from backups within the recovery objectives."

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

- Develop a coordinated test plan for 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;

- Retain documentation including test plans and evidence of completion.

# SECTION II: Implementation Status of Prior Audit Findings and Recommendations

**Table I**

**Summary of Implementation Status of Audit Findings and Recommendations from the Performance Audit Report for Fiscal Years Ending 2020 and 2019[10]**

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| 1. | There were three methods that agencies could use to procure software: CitiBuy, Expenditure Authorizations, and Procurement cards (P-cards). The City has controls in CitiBuy to capture IT software procurements initiated by agencies. However, controls are not established for EAs and the controls to capture P-card purchases are limited. Agencies, acting outside of the IT procurement process, procuring software without BCIT approval may increase IT security risk for the City and also creates the possibility of obtaining software when software | We recommend the CIO:<br><br>• Confirm that the Workday system has adequate controls to reduce the risk of agencies bypassing BCIT's IT procurement review process; and<br><br>• Notify the DOF to modify the audit of monthly P-card Statements to include software procurement transactions to confirm agencies obtained BCIT's approval for software procurements such as reviewing full details of transactions from the credit card company. | **Implemented**<br><br>In Workday when a requisitioner uses an IT spend category, the BCIT IT Spend Approver role is automatically added to the approval path of the requisition. The DOF has been notified and confirmed the implementation of the following policies and procedures implemented in August 2023. The DOF now requires all P-card holders to complete the procurement card program user guide training before a P-card is issued. The following purchases are also restricted at the credit card level: Electronic Purchases<br><br>• The purchasing of the electronic items listed below should be purchased via the purchase order process. If there isn't an active | **Implemented** |

[10] The objective of prior audit was to evaluate whether the City has adequate policies and procedures to guide the IT procurement processes to increase the efficiency and effectiveness of IT operations and costs.

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| | that already exists in the City would be an equal or better option. | | contract, then an approved BCIT waiver must accompany a P-Card Waiver for purchase approval:<br>o Computers<br>o Software<br>o Tablets<br>o iPad<br>o Televisions<br>o Gaming Systems<br>o Any item that has a USB that will connect to a City device.<br>• Memberships and Subscriptions – Agencies must submit and receive from the Bureau of Procurement an approved Waiver Request if these subscriptions are for electronic programs / applications a BCIT waiver approval must accompany the P-Card waiver request. Additionally, the above transactions are restricted at the card level under code 5045. The DOF completes monthly audits of P-card transactions. | |

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| 2. | While conducting the BCIT Biennial Performance Audit, the Applications (Apps) personnel stated that they maintain a list of City applications. This list will be used to determine if an agency purchase has the same functionality as other City existing applications. The Department of Audits requested a copy of a list of City applications, but to date, Apps was unable to provide a list. Even if Apps would have had an inventory list, it could only have captured applications that were given to Apps. According to BCIT personnel, the IT software procurement review process was established around October 2020. City agencies may have procured applications before this time; however, BCIT may not have captured all of them. For some applications that were procured before October 2020, BCIT may capture and perform an IT application procurement review when it is renewed, which may be included in BCIT's inventory list. | We recommend the CIO:<br><br>• Develop a complete inventory of all business-critical applications; and<br><br>• Establish the formal (written, dated, signed) City-wide policies and procedures outlining the roles and responsibilities of Apps regarding the maintenance of the application inventory and enforcing best practices around upgrades, planning, remediation, business continuity, and rationalization | **Partially Implemented**.<br><br>The BCIT has developed the inventory of applications on network. BCIT is in the process of modifying AM-301 as the initial step to establish formal City-wide policies and procedures. | **Partially Implemented.**<br><br>The development of a complete inventory of all business-critical applications is addressed in the current audit as part of Finding II (see page 7).<br><br>The BCIT still lacks Citywide policies and procedures outlining the roles and responsibilities regarding the maintenance of the application inventory and enforcing best practices around upgrades, planning, remediation, business continuity, and rationalization. |

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| 3. | Currently, according to the Infrastructure personnel, they use their institutional knowledge to review the requisitions for IT procurement and make the decision whether they need to notify Information Security (InfoSec) and / or Apps for their reviews. Additionally, once CitiBuy alerts BCIT Infrastructure personnel for review, the decisions whether to route requisitions to InfoSec and / or Applications for their reviews were not documented. This is because the BCIT Infrastructure does not have formal (written, approved, dated) policies and procedures for documentation of IT software procurement review process. | We recommend the CIO:<br><br>• Require the Infrastructure Functional Area to document their decisions whether to route requisitions to InfoSec and / or Applications for their reviews; and<br><br>• Establish formal (written, approved, and dated) policies and procedures to include this requirement. | **Implemented**.<br><br>A formal decision tree/process to determine when the InfoSec or Apps leadership was required for additional procurement approvals for requests within the CitiBuy procurement application is not documented. The decision to forward requests to the InfoSec and Apps teams' leadership was determined using the following criterium:<br><br>1. Did the request involve data that could be classified as having potentially "sensitive data", e.g. Personal Identifiable Information, Personal Health Information, Criminal Justice Information Services, etc. that would enter, exit or traverse the city's managed network resources?<br><br>2. Was the request unfamiliar with the Director of Infrastructure (new requests)?<br><br>3. Was the request submitted for a renewal of a software/maintenance/contract of an application or system?<br><br>In FY 2023, CitiBuy is no longer used as the mechanism for procurement requests, as Workday has been implemented and the procurement | **Implemented** |

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| | | | process was transitioned from CitiBuy into Workday. This change in the procurement system and process resolved the routing decision, from the sole delegate (Director of Infrastructure) in CitiBuy, to include the Chief Information Security Officer (CISO) and the Director of Infrastructure by default. In addition, either the CISO or the Director of Infrastructure adds the Director of Applications to all of the purchases for approvals; captured in the Workday system. Therefore, BCIT has resolved this finding. | |

| No. | Finding | Prior Recommendation | Management's Self-reported Implementation Status | Auditor's Assessment |
|---|---|---|---|---|
| 4. | The City's AM Sections for Computer Systems and Services are outdated and are not reflective of the current practices, creating ambiguity. Specifically,<br><br>• Outdated Policy: The City's AM 301-10, *Computer Systems and Services* (AM 301-10) and AM 301-10-1, *Computer Systems and Services Procedures* (AM 301-10-1) are out of date. The AM 301-10 and AM 301-10-1 address procurement and use of all computer systems and services including, but not limited to: consultants, hardware, software, training, maintenance, and grant applications which include computer systems and services.<br><br>• Ambiguous Policy: The AM 301-10 and AM 301-10-1 are not clear whether they address only those software procurements ($5,000 and above) that will go to BOE.<br><br>• Inconsistent Policy with the Current Practices: If AM 301-10 and AM 301-10-1 are interpreted as only those software procurements ($5,000 and above) that will go to BOE, then the AM 301-10 and AM 301-10-1 are not reflective of the current City's practices for all software procurements. | We recommend the CIO work with the Director of DOF, who is currently responsible to implement the AM 301-10 and AM 301-10-1, to:<br><br>• Update the AM 301-10 and AM 301-10-1;<br><br>• Communicate the updated AM 301-10 and AM 301-10-1 to City employees;<br><br>• Enforce the AM 301-10 and AM 301-10-1; and<br><br>• Revise the AM 301-10 and AM 30110-1 periodically. When the AM 301-10 and AM 301-10-1 are updated, consider including the industry standards such as National Institute of Standards and Technology and Federal Acquisition Regulations | **Partially Implemented**.<br><br>The BCIT is in the process of modifying AM-301-10 as the initial step to establish formal City-wide policies and procedures. | **Not Implemented.**<br><br>The current AM 301-10 draft does not address the procurement process. |

## APPENDIX I

# Management's Response to the Audit Report

**Date**: June 27, 2024

**To**: Josh Pasch, City Auditor

**Subject**: Management Response to Audit Report:
Biennial Performance Audit Report on Baltimore City Information Technology for the Fiscal Years Ended June 30, 2022 and 2021

Our responses to the audit report findings and recommendations are as follows:

**Recommendation I**

We recommend the CIO re-evaluate, update, formalize, and implement consultant's DRP recommendations to be reflective of current and future City computing environment. This plan should contain realistic DRP assumptions, appropriate technical recovery procedures and meet requirements of agency COOPs.

**Management Response/Corrective Action Plan**

**☒Agree ☐Disagree**

Due to the vast improvements that we have made to the City's technical environment since the 2019 Ransomware event, BCIT will engage with a consultant to update the DRP with the following milestones:

- By end of Q3 FY 2025: Engage with a consultant to update DRP; and
- By end of Q1 FY 2026: Consultant will provide a final DRP. At that time BCIT will develop a plan to implement those updated recommendations.

**Responsible Personnel:**

- Bruce Gibbons, Director of Infrastructure

## Recommendation II

We recommend the CIO conduct meetings with the respective City agencies and Mayoral offices to:

- As part of the development of DRP, 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 as, when agencies' applications are backed up by third party vendors or if agency IT units are in place.

We also recommend the CIO to work with the Chief Administrative Officer and the Director of Finance and OEM to update Administrative Manual guidelines (e.g., AM-110-1 *Continuity of Operations Plan*) to incorporate requirement for agencies to develop BIA in coordination with BCIT.

**Management Response/Corrective Action Plan**

**☒Agree ☐Disagree**

The BCIT will establish governance and oversight for disaster recovery that includes both BCIT-managed and agency-managed applications, and engage a consultant to update the DRP with a complete list of critical applications per the following milestones:

- By end of Q3 FY 2025: Engage a consultant to update the DRP; and establish Charter Disaster Recovery Governance Committee that includes agencies who manage their own IT applications; and
- By end of Q1 FY 2026: Consultant will provide a final DRP and as part of that an updated list of critical applications.

**Responsible Personnel:**

- Bruce Gibbons, Director of Infrastructure
- Robert McBride, Director of Applications

Additionally, BCIT will coordinate with OEM, the City Administrator, and DOF to update AM-110-1 *Continuity of Operations* to incorporate a requirement for agencies to develop a BIA as part of their COOP and that they consult BCIT as part of their BIA development. This will be completed by the end of FY2025.

## Recommendation III

We recommend the CIO:

- Develop a 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.

**Management Response/Corrective Action Plan**

**☒Agree ☐ Disagree**

BCIT will develop a cost-effective coordinated test plan for all critical City applications, perform restoration testing and coordinate resolution of issues identified during testing. Testing of Categories 1 and 2 applications will be contingent upon the development of a revised DRP. Milestones are as follows:

- By end of Q3 FY 2025: Engage with a consultant to update DRP;
- By end of Q4 FY 2025: Test Category 0 applications;
- By end of Q1 FY 2026: Consultant will provide a final DRP. At that time, BCIT will develop a plan to implement those updated recommendations; and
- By end of Q4 FY 2026: Test Categories 1 and 2 applications.

**Responsible Personnel:**

- Bruce Gibbons, Director of Infrastructure
- Robert McBride, Director of Applications