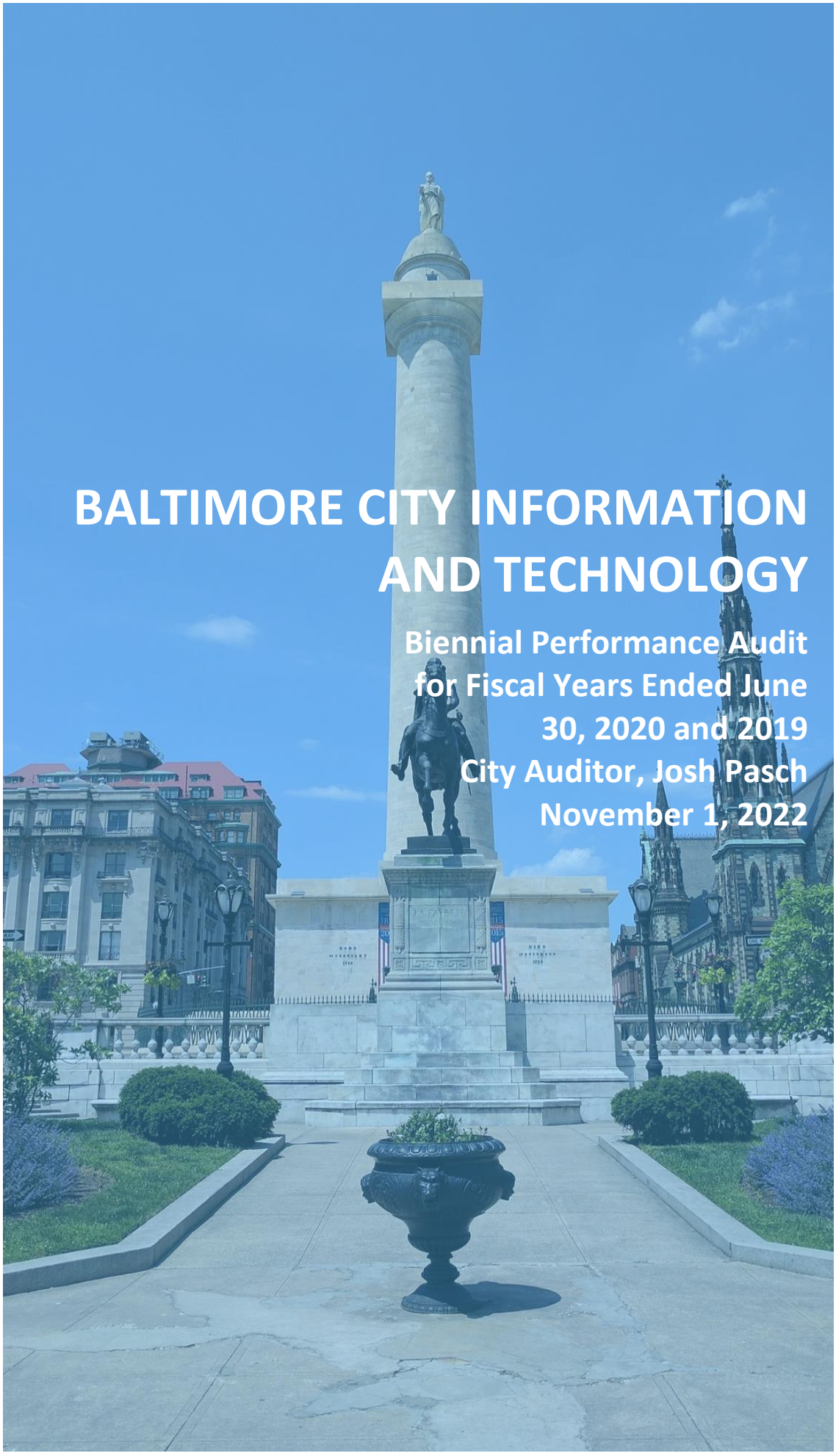


BALTIMORE CITY INFORMATION AND TECHNOLOGY

Biennial Performance Audit for Fiscal Years Ended June 30, 2020 and 2019

City Auditor, Josh Pasch

November 1, 2022

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, 2020 and June 30, 2019*. The objectives of our performance audit were to: (1) evaluate whether the City of Baltimore (City) has adequate policies and procedures to guide the City's Information Technology (IT) procurement processes to increase the efficiency and effectiveness of IT operations and costs; and (2) follow-up on findings and recommendations that were included as part of the previous performance audit report of Baltimore City Information and Technology (BCIT), dated September 4, 2019. The scope of our audit is fiscal years (FYs) 2020 and 2019; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify information during the audit period. Our focus is on software procurements only.

Our review indicated that the City and BCIT established an IT software procurement review process in October 2020. However, there remains the possibility of purchasing software that has the same functionality as other City existing software when an equal or better option exists. The following summarizes our findings:

- Agencies have opportunities to bypass the BCIT IT software procurement process when agencies choose to use Expenditure Authorizations[1] (EAs) and procurement cards (P-cards);

- BCIT's Applications Functional Area (Apps) currently does not have a complete list of City-wide applications[2] inventory;

- BCIT's Infrastructure Functional Area (Infrastructure) personnel are operating based on their institutional knowledge when making decisions whether to route agencies' software procurement requests to Information Security Functional Area

[1] EAs may be used for certain purchases: (1) purchases up to $5,000 of a Non-Recurring Nature; (2) obligations approved by the Board of Estimates (BOE) of a non-recurring nature; or (3) special authority uses. Special authority uses are certain specific categories of obligations that may be paid, even on a recurring basis and regardless of dollar amount, with an EA without seeking BOE approval for the payment. There are explicitly defined special authority uses in the Administrative Manual (AM) Section 303-1, *Expenditure Authorizations* (AM 303-1). The City discontinued EAs in Workday Financial Management, which was implemented in August 2022.

[2] Applications are categorized as Commercial-off-the-shelf (COTS), Software as a Service (SaaS), and Internally Developed

(InfoSec) and Apps to review. Infrastructure currently does not have formal (written, dated, and approved) policies and procedures; and

- The City's Administrative Manual (AM) Sections for Computer Systems and Services are outdated and are not reflective of the current practices, creating ambiguity.

Of the two prior recommendations that we followed up as part of this Biennial Performance Audit (See Section II on page 15), all recommendations were fully implemented.

To improve the efficiency and effectiveness of the IT software procurement process, 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 BCIT's and Department of Finance's (DOF) cooperation extended to us during our audit.

Respectfully,

Josh Pasch

Josh Pasch, CPA
City Auditor
Baltimore, Maryland
November 1, 2022

Background Information

Baltimore City Office of Information & Technology

The BCIT provides sustainable infrastructure and technology to support and enhance City departments, communities, and businesses to meet City and mayoral goals. The BCIT has three Functional Areas related to our audit objective, which play important roles in the IT software procurement review process: Infrastructure, InfoSec, and Applications.

- Infrastructure: The Infrastructure is responsible for the City's network servers, the data storage, and collaboration environment, such as Teams exchange. Additionally, Infrastructure is responsible for operating the service desk, which is the frontline interface to the end users of the City.
- Information Security: The InfoSec focuses on the discovery of cyber threats, characterization, and attribution of those threats, creation, and sharing of situational awareness, and the development of mitigation strategies. The mission of InfoSec is to support the City's agencies, departments, and personnel by safeguarding the confidentiality, integrity, and availability of City owned information. Housed at BCIT, InfoSec is currently responsible for developing the City's security policies, and increasing security awareness for the City's agencies, departments, personnel, and citizens.
- Applications: The Apps is focused on: (1) developing an understanding of various applications being purchased; and (2) reviewing whether the purchase overlaps with other current applications and how the potential purchase will integrate with other applications. During negotiation with the vendor, Apps will evaluate: (1) pricing and annual increase; and (2) favorable data ownership terms for the City.

BCIT Roles in IT Software Procurement Review Process

The IT software procurement review process was implemented by BCIT in October 2020. There were three methods that agencies could use to procure software: CitiBuy, EAs, and P-cards.

- **CitiBuy:** Requisitions were initiated by City-requesting agencies through CitiBuy to purchase software. CitiBuy was programmed with National Institute of Governmental Purchasing (NIGP)[3] codes that notified and routed requisitions to BCIT for approval. After agencies had completed requisitions, Infrastructure personnel received emails requesting action to begin the process to approve or deny requisitions. (Note: The City discontinued CitiBuy and implemented Workday Financial Management in August 2022.)
- **Expenditure Authorizations:** The BCIT reviewed software requisitions that were procured through EAs only when agencies requested BCIT's review.

[3] NIGP is a coding system primarily used to identify descriptions for goods and services.

- **Procurement Cards:** Agencies fill out a form and send it to the email account bcit.procurements@baltimorecity. The BCIT administrative staff have access to this email account and they forward the form to Infrastructure, InfoSec, and Apps.

For all procurement methods except P-cards, the IT software procurement review process starts with Infrastructure personnel. Based on the decision made by the Infrastructure personnel, the request for approval is forwarded to either InfoSec, Apps or both (see Exhibit I on page 5). For P-cards, BCIT administrative staff forward the request to Infrastructure, InfoSec, and Apps for their approval (see Exhibit II on page 5).

- **InfoSec's Review:** Upon receipt of the requests, InfoSec creates incident tickets in SolarWinds[4]. InfoSec then contacts the requestors with a series of questions related to sensitive information (e.g., Personal Health Information, Personal Identifiable Information, Criminal Justice Information, etc.) and whether the data will be transmitted and stored outside of BCIT's network. If the answers to all of the questions are yes, then InfoSec will perform IT software procurement reviews on those requests. These reviews consist of requesting System and Organizational Control[5] (SOC) 2 type II reports if available, or obtaining answers for IT security questionnaires (Contracts Information Security Rider; SR) which are sent to the vendors. Answers to these questions will help determine if the City's sensitive data is secured and protected. If the answers to the SRs and / or the SOC 2 type II reports are acceptable to BCIT standards, then the requests will be recommended for approval by InfoSec. If further clarification is needed, InfoSec will call the vendors and review any questions that need clarification. InfoSec will resolve the SolarWinds tickets with a recommendation for approval or denial.
- **Apps' Review:** According to Apps, it has a listing of applications and their functions in an "application inventory" (in-house Excel document), which is used to identify if an agency purchase has the same functionality as other City existing applications.
- **Administrative Staff's Approval:** For P-cards, once Infrastructure, InfoSec and Apps give their approval, the administrative staff will sign the completed form and return it to the requesting agency. Upon BCIT's approval, Bureau of Procurement (BOP) will issue a waiver that will unlock the P-card procurement.

[4] SolarWinds is BCIT's universal ticketing system that started in October 2020 to log and track incident tickets for security.

[5] SOC 2: (1) includes auditing procedures that ensure service providers securely manage data to protect the interests of an organization and the privacy of its clients; and (2) defines criteria for managing customer data based on five "trust service principles" – security, availability, processing integrity, confidentiality and privacy. There are two types of SOC 2 reports. A type I report on management's description of a service or organization's system and the suitability of the design of controls. A type II report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls. **Source:** American Institute of Certified Public Accountants

Exhibit I

Flowchart of IT Software Procurement Review Process for CitiBuy and EAs

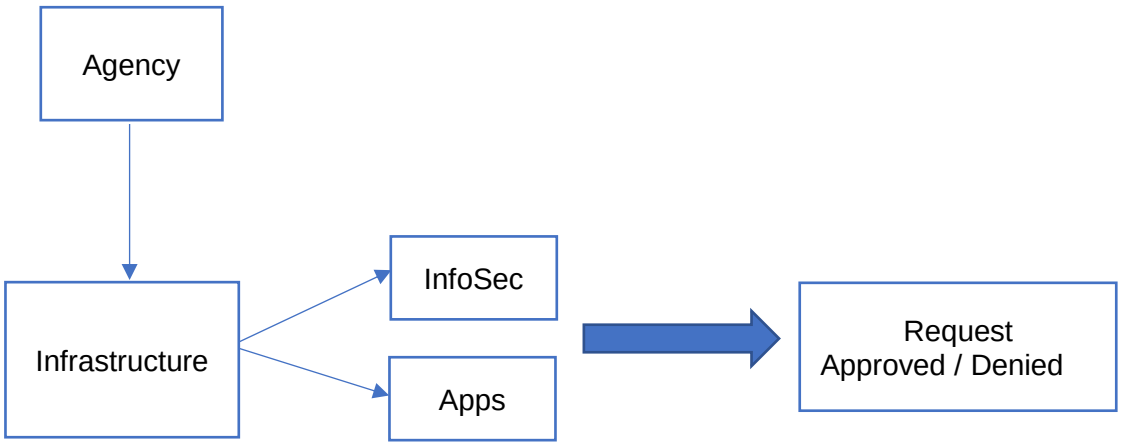
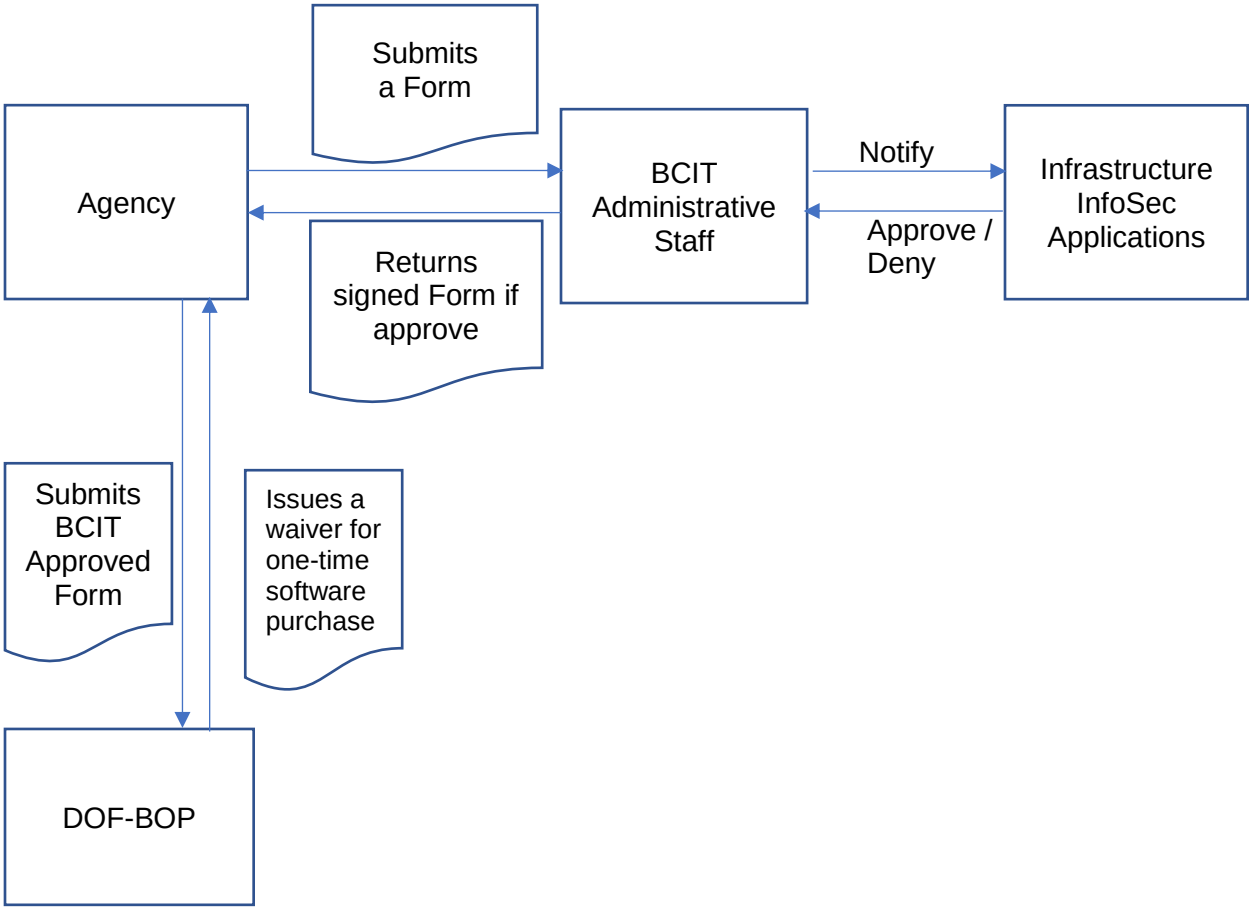


Exhibit II

Flowchart of IT Software Procurement Review Process for P-Cards



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 City has adequate policies and procedures to guide the City's IT procurement processes to increase the efficiency and effectiveness of IT operations and costs; and

- Follow-up on prior findings and recommendations included in the previous Biennial Performance Audit Report, dated September 4, 2019.

The scope of our audit is FYs 2020 and 2019; however, certain other matters, procedures, and transactions outside that period were reviewed to understand and verify the information during the audit period. Our scope is limited to software procurement only.

To accomplish our objectives, we:

- Identified and reviewed applicable standards that included documents published by the: (1) U.S. General Services Administration (GSA); (2) National Institute of Standards and Technology (NIST)[6]; (3) U.S. Government Accountability Office; (4) Information Systems Audit and Control Association; and (5) Information Resources Management College to identify criteria applicable to the audit objective;

- Reviewed applicable sections of the AM, including: (1) AM-303-1; (2) AM-309-1, *Small Purchases Procurement Card Program*; (3) AM-301-10, *Computer Systems and Services* (AM 301-10); and (4) AM-301-10-1, *Computer Systems and Services Procedures* (AM 301-10-1);

- Interviewed with and / or inquired of key personnel from the following departments to obtain an understanding of the processes, procedures, and internal controls related to the IT software procurement process: BCIT, and the following DOF bureaus: BOP, Treasury and Debt Management, and Bureau of Accounting and Payroll Services (BAPS);

[6] 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.

- Identified the key risks and evaluated whether the City has effective internal controls to reduce the identified risks;

- Performed testing, recalculations, and verified accuracy of reporting to assess compliance, completeness, and effectiveness of the processes noted above.

SECTION I: Current Findings and Recommendations

Finding I: Agencies can bypass BCIT's IT software procurement review process for certain procurement methods.

As stated in the Background Information, there were three methods that agencies could use to procure software: CitiBuy, EAs, and 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 (see below). 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 that already exists in the City would be an equal or better option.

Procurement methods that allow agencies to bypass the IT review

- EAs: The BCIT reviewed software requisitions that were procured through EAs only when agencies requested BCIT's review. BAPS, a bureau of the DOF, reconciled purchase orders (POs), receipts, and invoices before making payments to vendors. However, they did not check whether POs related to software procurement had been previously approved by BCIT. According to DOF BAPS personnel, agencies should have already received BCIT's approval by the time BAPS received payment requests from agencies. (Note: The City ended using EAs in Workday Financial Management, which was implemented in August 2022.)

- P-cards: According to BOP, the software procurements on the City's P-cards are restricted by the Merchant Category Code (MCC). If agencies want to procure software, they must obtain BCIT's approval. Then, DOF BOP will issue a waiver to allow an agency to make that one-time software purchase. However, there is a residual risk that agencies can bypass the BCIT review. Specifically,

    - The MCC is assigned to a vendor. The assigned MCC may not be representative of all products offered by the vendor; as items not part of the MCC description can be procured from that vendor. For example, Amazon has an MCC with a description of "Books;" however, any item listed in the Amazon catalog can be procured. Therefore, there is a risk of procuring items from Amazon that are restricted under another MCC.

    - The BOP's monthly audit of the P-card statements may not capture software procurements. This is because BOP's sample selection methodology for 20-30 transactions a month is based on high volume of transactions or high-dollar amounts, which may or may not capture software procurements.

Polydys ML, Wisseman S (2008) *Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing*. (National Defense University Press, Washington, D.C. Information Resources Management College[7] Occasional Paper) states that:

- Software Assurance Requirements. "…Acquirers developing acquisition strategies and plans should rely heavily on the Software Assurance (SwA) personnel assigned to the acquisition." For example, to ensure that Commercial-off-the-shelf (COTS) software consistent with the overall security requirements of the software-intensive system, SwA personnel assigned to this acquisition will provide requirements to ensure delivery of COTS software that has specified preset security settings. In addition, requirements will mandate that testing of the specified preset software be accomplished on the operating system and platform proposed for production.

- Software Assurance Considerations in Contractor Selection: "High-level statements should be included in acquisition strategies and plans on how SwA will be considered in the selection of contractors. For example, "due-diligence questionnaires will be used to solicit answers from offerors on their SwA practices." The due-diligence questionnaires should be part of the evaluation plan."

Recommendation I: We recommend the CIO:

- Confirm that the Workday system has adequate controls to reduce the risk of agencies bypassing BCIT's IT procurement review process; and

- Notify the Director of 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.

[7] "The College is a National Center of Academic Excellence in Information Assurance Education designated by the Department of Homeland Security and National Security Agency."

Finding II: The Applications Functional Area does not have processes and a system to identify, record, update, and maintain a centralized inventory of all the City's business-critical applications.

While conducting the BCIT Biennial Performance Audit, the 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.

Background Information About Application Inventory

In order to keep business operations working as efficiently as possible, an organization should maintain an application inventory to support:

- Management of upgrades and patches
- Operational and financial planning
- Remediation of security issues
- Business Continuity testing and recovery
- Application rationalization

Source: BCIT

A lack of a complete and accurate list of City applications may increase the risk of the City not being able to effectively manage the items listed in the text box. Additionally, BCIT is not aware of applications that they can patch, update, or secure properly to reduce the risk of a cyber-intrusion.

The cause of this finding is there are no City-wide formal policies and procedures outlining the roles and responsibilities of Apps for recording and maintaining a list of City applications.

The NIST Special Publication NIST SP 800-161r1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* state:

- "Enterprises may choose to implement centralized inventories that include components from all enterprise information systems, networks, and their components. Centralized repositories of inventories provide opportunities for efficiencies in accounting for information systems, networks, and their components. Such repositories may also help enterprises rapidly identify the location and responsible individuals of components that have been compromised, breached, or are otherwise in need of mitigation actions."

- "When installing, updating, or removing an information system, information system component, or network component, the enterprise needs to update the inventory to ensure traceability for tracking critical components."

Recommendation II: We recommend the CIO:

- Develop a complete inventory of all business-critical applications; and

- 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.

Finding III: There Is No Audit Trail for BCIT Infrastructure Functional Area's Decisions for IT Procurement Review.

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 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.

As a result, without Infrastructure personnel's assistance, it is not possible to substantiate the rationale that Infrastructure uses to determine whether a requisition is sent to InfoSec, Applications, or neither. For example, for FY 2022 up to June 8, 2022, there were 451 software-related requisitions in CitiBuy. However, in SolarWinds, which is a ticket-tracking system for InfoSec review, only 58 of these were routed to or researched by InfoSec. According to the BCIT Infrastructure personnel, the remaining 393 requisitions were not reviewed because these requisitions were related to existing software renewals and City pre-approved vendors or products (e.g., LexisNexis, Microsoft and Adobe).

According to the *Standards for Internal Control in the Federal Government issued by the Comptroller of the United States* (Green Book), "documentation is a necessary part of an effective internal control system…Documentation is required for the effective design, implementation, and operating effectiveness of an entity's internal control system."

Recommendation III: We recommend the CIO: (1) require the Infrastructure to document their decisions whether to route requisitions to InfoSec and / or Apps for their reviews; and (2) establish formal (written, approved, and dated) policies and procedures to include this requirement.

Finding IV: The City's Administrative Policies Related to Computer Systems and Services Are Outdated, Ambiguous, and Inconsistent with Current Practices.

The City's AM Sections for Computer Systems and Services are outdated and are not reflective of the current practices, creating ambiguity. Specifically,

- **Outdated Policy**: The City's AM 301-10 and 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. The last update for both AM 301-10 and AM 301-10-1 was May 18, 2012.

- **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. Since the AM 301-10 and AM 301-10-1 appear to address only those software procurements ($5,000 and above) that will go to BOE, some individuals may think that they do not have to obtain BCIT's approval for software procurements less than $5,000 if they are using EAs. This results in a security risk for software procured under $5,000.

- **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. Currently, as stated in the Background Information, BCIT is reviewing software procurements that are referred by CitiBuy. In CitiBuy, the referral is based on NIGP Commodity Codes that identify descriptions for goods and services. For any software procurements on P-cards, agencies must obtain BCIT's and BOP's approvals and waivers.

Formal periodic review of policies and procedures promote compliance, accountability, consistency, and continuity. According to the Green Book, management:

- Documents in policies the internal control responsibilities of the organization;

- Communicates to personnel the policies and procedures so that personnel can implement the control activities for their assigned responsibilities; and

- Periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology.

Recommendation IV: We recommend the CIO work with the Director of Finance, who is currently responsible to implement the AM 301-10 and AM 301-10-1, to: (1) update the AM 301-10 and AM 301-10-1; (2) communicate the updated AM 301-10 and AM 301-10-1 to City employees; (3) enforce the AM 301-10 and AM 301-10-1; and (4) revise the AM 301-10 and AM 301-10-1 periodically. When the AM 301-10 and AM 301-10-1 are updated, consider including the industry standards such as NIST and GSA's Federal Acquisition Regulations.

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 2018 and 2017 for Service 804 – 311 Call Center[8]

No.	Finding	Prior Recommendation	Management's Self-reported Implementation Status	Auditor's Assessment
1.	The BCIT was unable to provide documentation to support actual amounts of the selected performance measures reported in the Budget Books. One of the responsible personnel's hard drive was confiscated and the other responsible personnel's selected files were removed due the May 2019 ransomwares incident.	The CIO of BCIT require that the Service 804 periodically: (1) back up data; and (2) perform tests and recovery of historical and backup data.	**Implemented**. BCIT established a SharePoint site used to input our monthly performance metrics and the associated back up. The SharePoint site is part of the Microsoft cloud-based system and is backed up on a daily basis.	**Implemented.**

[8] The selected performance measures are Average Time to Answer a 311 Call (seconds), Percent of 311 Calls Answered within 60 Seconds and Number of Calls Received in 311.

No.	Finding	Prior Recommendation	Management's Self-reported Implementation Status	Auditor's Assessment
2.	A target for this measure cannot be reasonably established because such target and its achievements are beyond BCIT's control. Specifically, the number of calls received by the 3-1-1 Call Center is solely based on residents' calls for any given period and is not controllable by the 3-1-1 Call Center. As a result, this performance measure does not effectively measure the 3-1-1's productivity in serving 3-1-1 service requests. In addition, there is no clear link of action to be taken as a result.	The CIO of BCIT modify the performance measure as the percentage of calls answered by 3-1-1 (the number of calls answered by 3-1-1/the number of calls received by 3-1-1) to reasonably measure 3-1-1's productivity in serving 3-1-1 service requests.	**Implemented**. Percent of calls answered within 60 seconds is a measure tracked in the annual Bureau of the Budget and Management Research (BBMR) Budget Book. While number of calls received in 311 continues to be a measure tracked in the annual BBMR Budget Book, starting in FY2021, there is no longer a target for that measure. It is incorporated only for context purposes for the other 311 measures.	**Implemented.**

APPENDIX I

Management's Response to the Audit Report

Date: October 25, 2022

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, 2020 and 2019

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

Recommendation I

We recommend the CIO:

- Confirm that the WD system has adequate controls to reduce the risk of agencies bypassing BCIT's IT procurement review process; and

- Notify the Director of 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.

Management Response/Corrective Action Plan

☒**Agree** ☐**Disagree**

BCIT agrees with the recommendation.

Implementation Date: Quarter IV of FY 2023

Responsible Personnel: BCIT Administration and Application Directors

Recommendation II

We recommend the CIO:

- Develop a complete inventory of all business-critical applications; and
- 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.

Management Response/Corrective Action Plan

☒Agree ☐Disagree

BCIT agrees with the recommendation

Implementation Date:

- Updated list of Applications – Quarter III of FY 2023
- Policies/Procedures - Quarter IV of FY 2024
    - Milestone: Implementation will be contingent upon the issuance of the revised AM-301 (see Finding IV). BCIT's plan for AM - 301 is to establish an IT Charter that points to an IT manual that BCIT will update, which is similar to Department of Human Resources and the Personnel Manual. The application policies referenced in Finding II will actually be standards within the IT manual; as a result, their issuance will be contingent upon modifying AM-301.

Responsible Personnel: BCIT Security and Application Directors

Recommendation III

We recommend the CIO: (1) require the Infrastructure Functional Area to document their decisions whether to route requisitions to InfoSec and / or Applications for their reviews; and (2) establish formal (written, approved, and dated) policies and procedures to include this requirement.

Management Response/Corrective Action Plan

☒Agree ☐Disagree

BCIT agrees with the finding that a formal decision tree/process to determine when the Information Security or Application leadership was required for additional procurement approvals for requests within the CitiBuy procurement application is not documented. The decision to forward requests to the Information Security and Application teams' leadership was determined using the following criterium:

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?

2. Was the request unfamiliar with the Director of Infrastructure (new requests)?

3. Was the request submitted for a renewal of a software/maintenance/contract of an application or system?

In FY23, CitiBuy is no longer used as the mechanism for procurement requests, as Workday has been implemented and the procurement 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.

Implementation Date: Q2 FY 2023

Responsible Personnel: BCIT Infrastructure Director

Recommendation IV

We recommend the CIO work with the Director of Finance, who is currently responsible to implement the AM 301-10 and AM 301-10-1, to: (1) update the AM 301-10 and AM 301-10-1; (2) communicate the updated AM 301-10 and AM 301-10-1 to City employees; (3) enforce the AM 301-10 and AM 301-10-1; and (4) revise the AM 301-10 and AM 301-10-1 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.

Management Response/Corrective Action Plan

☒Agree **☐Disagree**

BCIT agrees with the recommendation.

Implementation Date: Quarter IV of FY 2024

Milestones:

- By April 30, 2023, BCIT will draft revised policies.
- By August 30, 2023, share draft policy with BCIT's IT Security Council, receive feedback from members, and disposition all feedback.
- By December 30, 2023, share draft policy with agency directors and their deputies, receive feedback from members, and disposition all feedback.
- By February 28, 2024, share draft policy with the IT Citywide Governance Committee, receive feedback from members, and disposition all feedback.
- By March 31, 2024, prepare final policy and submit with memo to the Department of Finance.
- By May 31, 2024, policy revision approved by BOE.

Responsible Personnel: BCIT Security Director