Results in Brief

OIG-19-11
June 19, 2019

Why We Did This Review

This is the second report covering Washington Metro Area Transit Authority (WMATA's) management of software assets. The first report *Audit of WMATA's End-of-Service Life Operating System Software*, dated May 1, 2019 covered known operating system software which if left unaddressed and thereafter exploited could increase the opportunities for data breaches and vulnerability exploits.

The objective of this audit was to determine the adequacy of WMATA's Software Asset Management (SAM) Program.

A SAM Program provides centralized software management and administration. Software financial and operational data assist organizations to manage and navigate the risks and vulnerabilities associated with software lifecycle management and maintenance.

Audit of WMATA's Software Asset Management Program

What We Found

WMATA has not implemented a comprehensive SAM Program capable of managing software assets across the enterprise. WMATA developed some policies, informally assigned responsibilities, and conducted some scanning. However, other critical program requirements were not implemented including a software risk assessment, software resources, software inventory controls, detailed standard operating procedures, and quality assurance controls.

The Information Technology (IT) Department did not have a comprehensive SAM program because they first needed to centralize financial control of IT assets, better align IT resources, and develop baseline program policies. A comprehensive SAM program would allow WMATA to fully manage software, and lessen WMATA's risks of exposure to cyberattacks, data breaches, and other exploits.

Management's Response

WMATA's Executive Vice President of Internal Business Operations (EVP/IBOP) provided written comments dated May 31, 2019 (Appendix B). The EVP/IBOP concurred with the finding and recommendation; however, corrective actions will be a multiyear effort that will take until the end of Fiscal Year 2022 to fully implement. OIG considers management's comments responsive to the recommendation, and the planned corrective actions should correct the deficiencies identified in the report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ABBREVIATION	DESCRIPTION
CIO	Chief Information Officer
EOSL	End-of-Service Life
EVP/IBOP	Executive Vice President/Internal Business Operations
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
MIS	Management Information System
MITS	Metro Information Technology Security
OIG	Office of Inspector General
O/S	Operating System
P/I	Policy Instruction
SAM	Software Asset Management
SOP	Standard Operating Procedures
WMATA	Washington Metropolitan Area Transit Authority

BACKGROUND

SAM Program - A SAM Program provides centralized software management and administration. Software financial and operational data assist organizations to manage and navigate the risks and vulnerabilities associated with software lifecycle management/maintenance. The International Standards Organization (ISO) states that software asset management is "all of the infrastructure and processes necessary for the effective management, control and protection of the software assets within an organization, throughout all stages of their life cycle."

Microsoft states that "[s]oftware Asset Management (SAM) is a set of proven IT practices that unite people, processes, and technology to control and optimize the use of software across an organization. SAM can help you control costs as well as manage business and legal risks, optimize software licensing investments, and align your IT investments with business needs."

Organizational Alignment - The IT Department, under the Chief Information Officer (CIO), is responsible for managing the SAM Program.

Prior Audit Coverage - OIG issued the *Audit of WMATA's End-of-Service Life Operating System Software* on May 1, 2019, which concluded that WMATA's operating systems and contractor-owned systems were running end-of-service life operating system (O/S) software. The end of vendor support for the various O/S software had, in some cases, ended years earlier.

When vendors stop supporting older versions of their products, those products pose significant security risks because updates are no longer available. These vulnerabilities increase the opportunities for cyberattack, data breaches, and vulnerability exploits. If left unaddressed and thereafter exploited, these vulnerabilities could have monetary impacts, impair operations, endanger public safety, and damage WMATA's reputation. The OIG made recommendations to specifically address the known EOSL O/S software vulnerabilities, to which management concurred and provided corrective action that should correct the deficiencies identified in the report.

AUDIT OBJECTIVE AND RESULTS

Audit Objective

To determine the adequacy of WMATA's SAM Program.

Audit Results

WMATA has not implemented a comprehensive SAM Program capable of managing software assets across the enterprise. WMATA developed some policies, informally assigned responsibilities, and conducted some scanning. However, other critical program requirements were not implemented. (Refer to Table 1 and details are in Appendix C).

Table 1: Status of the SAM Program

SAM Program Requirements	Implemented/Under Development	Not Implemented
1. Project Plan		X
2. Software Asset Management Policy Instruction	X – policy in draft	
3. Related Policies with Software References	X	
4. Software Risk Assessment		X
5. Standard Operating Procedures (SOP)		X
6. Organizational Infrastructure	X – informally assigned responsibilities	
7. Management Information System (MIS) Capability		X
8. Software Inventory		X
9. Other Internal Controls – Quality Assurance and procurement controls		X
10. Scanning	X - fragmented	

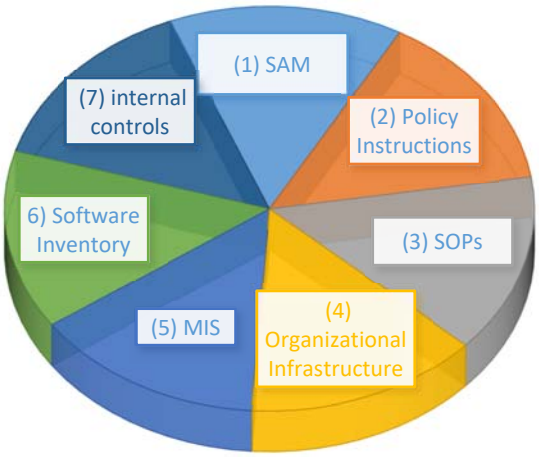
What Is Required

SAM is one of the most basic controls and a critical component to IT operations. The Center for Internet Security, Control 2: Inventory of Authorized and Unauthorized Software states: "Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution." It also states: "Inventory management can be challenging for any organization, but you can't protect your systems unless you know what's running on them."

WMATA's Draft Policy Instruction (P/I) *15.22/0, IT Asset Management* provides that Information Technology Asset Management is "[a] strategic and systematic process through which an organization procures, operates, maintains, rehabilitates, and replaces IT Assets to manage their performance, risks and costs over their lifecycle to provide safe, cost effective, reliable service to current and future Customers and for achieving its organizational strategic plan." WMATA also had assembled related software maintenance guidance in several P/Is – see Appendix D.

Best practices found in ISO/IEC (International Electrotechnical Commission) 19770-1:2017[1] and the Microsoft SAM Optimization Model[2] provide guidance on the elements of a SAM program – see Diagram 1.

Diagram 1 - Complete SAM Program Control/Elements[3]



Why This Occurred

The OIG found that actions taken by IT to implement a SAM Program and manage the lifecycle of software assets were random, ad hoc and unplanned. The CIO indicated they first needed to centralize financial control of IT assets, better align IT resources, and develop baseline program policies. The CIO stated controls over IT assets and staff realignment have been completed, and the asset management policy is in draft. The CIO also stated they are conducting a comprehensive enterprise risk assessment which would help focus on critical software assets. Management also stated they continue to align operational resources under IT, widening ITs' span-of-control over Metro's operational assets.

[1]International Standard, Information technology - IT asset management - Part 1: IT asset management systems – Requirements
[2]*Microsoft SAM Optimization Model* provides "The IO model is used to benchmark your organization's current Information Technology (IT) infrastructure and help create a more secure and better managed environment. The primary goals of IO are to help rationalize and reduce your IT costs, reallocate underutilized IT resources, and streamline IT business processes. Implementing SAM, which is an integrated set of policies, processes, people and tools dedicated to discovery and management of an organization's software holdings, is necessary so an organization can optimize its IT assets. Information technology optimization is a common goal of both the IO Model and the SAM Optimization Model, therefore it makes sense for your organization to align these initiatives along a common framework."
[3]Derived as a compilation of "best practice" recommendations.

Why This Is Important

When fully implemented, a comprehensive SAM program reduces the risks of exposure to cyberattacks, data breaches, and other exploits. It allows a business to fully manage software as an asset. This includes remediation of known systems running EOSL O/S software, developing a comprehensive inventory of software, and managing software licenses. A business implementing a comprehensive SAM program also reduces the likelihood of impacts on financial, operations, safety, and reputation.

Recommendation

We recommend to the General Manager/Chief Executive Officer:

1. Develop and implement a comprehensive SAM Program that corresponds with industry best practices. (Action: IBOP)

SUMMARY OF MANAGEMENT'S RESPONSE

WMATA's EVP/IBOP provided written comments dated May 31, 2019 (Appendix B). The EVP/IBOP concurred with the finding and recommendation; however, corrective actions will be a multiyear effort that will take until the end of Fiscal Year 2022 to fully implement. OIG considers management's comments responsive to the recommendation, and the planned corrective actions should correct the deficiencies identified in the report.

Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine the adequacy of WMATA's SAM Program.

Scope

This second report covers WMATA's management of software assets by examining the SAM Program. The first SAM review, entitled *Audit of WMATA's End-of-Service Life Operating System Software*, dated May 1, 2019 examined operating system software that had reached the end of its service life.

Methodology

To accomplish our audit the OIG:

1. Reviewed relevant documentation such as: policy instructions and best practices;

2. Interviewed employees from the IT Department including the CIO and Data Center and Infrastructure, Networks and Communications, IT Security, and Enterprise Architecture staff;

3. Evaluated the internal controls over the SAM Program;

4. Researched and analyzed SAM industry standards such as: ISO/IEC 19770-1:2017, Information Technology Infrastructure Library Application Management, and the Microsoft SAM Optimization Model.

We did not rely on computer generated data to accomplish our objective.

This audit was from May 2018 through April 2019 in accordance with generally 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 objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Appendix B

MANAGEMENT'S RESPONSE

M E M O R A N D U M

SUBJECT: Office of Inspector General (OIG) Audit of WMATA's Software Asset Management Program [redacted]

DATE: May 31, 2019

FROM: EVP/IBOP – John T. Kuo

THRU: GM/CEO – Paul J. Wiedefeld [redacted]

TO: OIG – Geoffrey Cherrington

WMATA's Executive Vice President of Internal Business Operations (IBOP) has prepared the following response to the Office of Inspector General (OIG) Audit of WMATA's Software Asset Management Program.

WMATA IBOP leadership has reviewed the memorandum and held preliminary discussions regarding OIG's recommendation with the office of Information Technology (IT). In the following memorandum, WMATA IBOP has detailed their initial plans to develop a Software Asset Management Program in line with OIG's recommendation.

IBOP leadership is confident in their current programs and processes and welcomes the opportunity to improve and enhance the software asset management program. IBOP concurs with the recommendation in the report and will proactively use OIG's recommendation to address the identified areas. The following corresponding actions will be taken by Metro IT to implement a holistic IT Asset Management Program to address the SAM related issues identified by OIG by the end of Fiscal Year 2022:

- Define a set of inventory attributes that maximizes the benefits of a central IT asset repository;
- Develop and maintain accurate IT Asset Inventories – Including hardware, software, network and security equipment;
- Coordinate with End of Service Life (EOSL) efforts to track IT asset replacement priorities; and,
- Develop supporting governance documentation of the IT Asset Management (ITAM) program.

Washington Metropolitan Area Transit Authority

OIG Recommendations & Management Response:

1. Develop and implement a comprehensive SAM Program that corresponds with industry best practices.

a. IBOP accepts this recommendation. WMATA acknowledges it has not implemented a comprehensive Software Asset Management (SAM) Program capable of managing software assets across the enterprise. As a part of its continued efforts to enhance operational efficiencies, Metro IT will implement a holistic IT Asset Management (ITAM) Program to address the SAM related issues identified by OIG.

In May 2018, the Metro IT produced a draft report "WMATA IT Software Asset Lifecycle Management Governance Model & Framework" that lays out a process to develop, maintain, and verify (through interviews and enterprise-wide scans) software asset inventories. Upon further analysis, Metro IT determined that addressing software assets may not be practical without also addressing systems architecture, hardware inventories, and software inventories due to the dependencies between them. These dependencies call for a comprehensive IT Asset Management (ITAM) and End of Life Software Refresh Program that is broader than SAM.

Among its expected outcomes, the proposed ITAM Program will address the OIG identified risks and weaknesses. Once approved, the Program will span three years and include the following activities:

- Defining a set of inventory attributes that maximizes the benefits of a central IT asset repository to fully manage these assets and lessen the risks of exposure to cyberattacks, data breaches, and other exploits
- Developing and maintaining accurate IT Asset Inventories – Including hardware (servers, data storage units, appliances, and end user equipment), software (Operating Systems, Database Management, Enterprise Resource Management, etc.), and network and security equipment (switches, routers, firewalls, Virtual Private Networks, etc.)
- Coordinating with End of Service Life (EOSL) efforts to track IT asset replacement priorities following a risk-based approach and supporting decisions to pursue replacement versus service consolidation for each technology refresh

Specifically, the ITAM Program will address the following weaknesses identified in Table 1 of the OIG's audit report:

- SAM Planning – Complete the formulation of a Project Plan with projected timelines, costs, risk management activities, and

milestones. This effort will identify funding sources to finance improvements, coordinate with EOSL efforts to track IT asset replacement activities, and coordinate with efforts to design, build, and transition to a new Metro datacenter as appropriate.

- SAM Policy Instructions – IT will finalize and request GM approval for an Enterprise ITAM policy. IT will also revise and submit updates, as appropriate, for other related policies, (e.g., P/I 15.21 Vulnerability Management P/I; P/I 15.15, Software License and Digital Rights Management Policy; and WMATA IT Security Standards and Guidelines), to ensure support for the ITAM Program.
- Standard Operating Procedures (SOP) – IT will develop and maintain procedures for the implementation of the ITAM Program, roles and responsibilities for registering and tracking IT assets, licenses and monitoring warranties, and support services such as inventories, scanning, risk assessment, etc.
- Organizational Infrastructure Formulation – IT will formally define a governance structure for ITAM, which will be reflected in the SOP. This structure will identify stakeholders and define an appropriate RACI Matrix.
- Information Management Tool Implementation – IT will design a management tool and repository for ITAM. The tool will maintain a set of inventory attributes to maximize the benefits of maintaining this central repository. The tool will maintain accurate IT Asset Inventories to include hardware (servers, data storage units, appliances, and end user equipment), software (Operating Systems, Database Management, Enterprise Resource Management, License Management, etc.), network and security equipment (switches, routers, firewalls, Virtual Private Networks, etc.), Operational Technology (OT), and embedded devices as appropriate.
- Related Internal Control Activities – IT will define ancillary controls activities through policy instructions and implement them as appropriate through, SOPs and automated mechanisms such as scanning tools to maintain quality assurance, procurement controls, and risk assessment/management.

As this is a multi-year effort, IBOP will provide OIG an update on June 1, 2020.

Appendix C

SUMMARY OF SAM PROGRAM REQUIREMENTS

SAM Planning – WMATA had not developed a formal SAM Program implementation plan which outlined project requirements, such as: scope, schedule, cost, quality, staffing, communication, risks, activities, tasks, and milestones.

Comprehensive SAM Program Policy Instructions – WMATA had not developed and implemented a comprehensive SAM P/I. WMATA provided the Information Technology Asset Management P/I. However, the P/I was in draft and the IT Department management stated they did not know when the policy would be approved. Further, the IT Department provided P/I 15.21 Vulnerability Management P/I; P/I 15.15, Software License and Digital Rights Management Policy; and WMATA IT Security Standards and Guidelines. These policies contain elements found in a SAM Program.

SOPs and Policies – WMATA had not developed SOPs to guide the various IT offices in performing their respective SAM Program activities.

Organizational Infrastructure Formulation – WMATA management had not formally defined the organizational infrastructure, reporting relationships and responsibilities, and tasks required to manage a SAM Program. WMATA had not developed a responsible, accountable, consulted, and informed (RACI) matrix which would demonstrate organizational relationships. The IT Department representatives stated IT was currently in the process of developing the requisite organizational infrastructure.

MIS – WMATA had not implemented a MIS capable of managing WMATA software assets. A SAM Program MIS would centralize pertinent software asset data to allow management of the asset throughout its useful life. The IT Department management stated IT had not implemented an automated system, but had begun the process to identify an automated solution.

Software Inventory Control – WMATA was not able to provide a comprehensive enterprise-wide software inventory. The IT Department has hardware and software discovery tools. However, throughout the enterprise, hardware and software is not configured to allow those tools visibility into all systems. The IT Department offices had some visibility into systems they either managed, deployed, or had the opportunity to install discovery agents. Additionally, the IT Department representatives stated "shadow IT systems" exist within WMATA. Shadow IT systems are systems not managed by the IT Department and that IT may not have visibility.

Other Internal Controls Activities: WMATA had not developed corresponding internal controls structures to support the SAM Program including:

- *Risk Assessment Activities* – WMATA does not have a fully structured and operational enterprise IT Risk Management Program which would include software asset management.
- *Quality Assurance Activities* – WMATA had not commenced activities to remedy incidents of known software vulnerabilities. IT managers tasked with taking actions to remedy "out-of-service life" software stated they were aware of the issue; however, no actions had been taken.
- *Procurement Planning/Coordination* - WMATA required that all IT procurements be approved by the IT Department. However, neither the IT managers that approved requests, nor procurement; track the software at receipt or deployment.

Scanning

- *Vulnerability Scanning* – WMATA's software asset scanning was fragmented. Several of the IT offices were generally responsible for scanning the systems they had visibility and managed.

Appendix D

SAM PROGRAM BEST PRACTICES AND WMATA PROVISIONS

SAM PROGRAM REQUIREMENT	ISO/IEC 19770-1 PROVISIONS	MS IO MODEL[4]	WMATA REQUIREMENT[5]
Software Asset Management Planning	Sections: 3.27 (Definition), 4.1 - 4.4, 5.1, 6.1, 6.2	Yes	No requirement.
Policy Instructions and SOPs	Section 5.2, 8.1	Yes	P/I 15.21, *Vulnerability Management Policy*, section 4.03(a) provides "[d]evelop and publish procedural guidance on patch management, vulnerability management, and system hardening."
			P/I 15.22/0, *IT Asset Management*, Draft section 4.02(a) "standardizing processes, procedures, tools **[MIS]**, and guidelines to promote consistent management of Metro's IT Assets throughout their useful life, and to allow customers to understand their roles and responsibilities."
	Sections: 8.1, 8.4	Yes	P/I 15.21, section 5.01(c) and "provides that all system devices belonging to or managed by metro will have the latest Services Packs and Security Patches installed."
	Section 10	Yes	P/I 15.21, section 4.01(e) provides "[w]ork with MITS to develop and maintain a Metro vulnerability remediation database and set priorities for all known Metro vulnerability remediation efforts."
Organizational Structure Formulation	Sections: 3.33, 5.3, 6.2, 7, 8, 8.8	Yes	No requirement
Management Information System Requirement	Sections: 7.5, 7.6, 8.3	Yes	No requirement
Software Inventory	Sections: 8.4, 8.5	Yes	P/I 15.21, section 4.01(c) provides "[c]reate and maintain system inventories of all Metro Technology Assets under their purview . . . and maintain updated records within the MITS risk repository."
			P/I 15.21, section 4.02(b) provides "[e]nsuring that information about Metro's IT Asset portfolio is complete and up to date."
			P/I 15.22/0, *IT Asset Management*, Draft section 4.02(b) provides that IT has the authority and responsibility for "[e]nsuring that information about Metro's IT Asset portfolio is complete and up to date."
Internal Control Structures - Risk Assessment Activities	Sections: 6.1.2 , 6.1.3, 8.2	Yes	P/I 15.21, section 4.01(c) provides ". . . maintain updated records within the MITS risk repository."
			WMATA IT Security Standards and Guidelines, Office of Chief Information Security Officer, Standards Description Document, IT-MITS-STND-01, Version 1.0 provides that MITS is responsible for IT risk management activities.
Internal Control Structures - Quality Assurance Activities	Sections: 7.6.3, 8.5, 9.2, 9.3	Yes	P/I 15.21, section 4.0(d) provides "[a]udit systems for vulnerabilities on a Metro-wide basis to ensure vulnerability management remediation is occurring."
Internal Control Structures - Vulnerability Scanning	Sections: 8.5, 10.2	Yes	P/I 15.21, section 4.01(h) provides "[c]onduct vulnerability scans to ensure remediation solutions and patches have been successfully deployed to Metro's production environments."
Procurement Planning and Coordination			No requirement

[4] *Microsoft SAM Optimization Model*

[5] SAM Program elements contained in various P/Is and other guidance.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: wmata-oig-hotline@verizon.net

Telephone: 1-888-234-2374

Address: WMATA
Office of Inspector General
Hotline Program
600 5th Street, NW, Suite 3A
Washington, DC 20001