THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Board Report

Office of the General Auditor

- **General Auditor's Report for December 2025**

Summary

This report highlights significant activities of the Office of the General Auditor for the month ended December 31, 2025.

Purpose

Informational

Attachments

Two reports were issued during this period:

1. Cybersecurity Audit: Inventory & Control of Operational Technology Assets
2. First Follow-up Review: Check with Order

Detailed Report

<u>Audit & Advisory Projects</u>

Twenty-three projects are in progress:

- Eight audit projects are in the report preparation phase.
  - One collaboration draft report was issued: Contract Audit: California Landscape Contractors Association
- Fourteen projects are in the execution phase, including five audits and nine advisories.
- One project is in the planning phase.

No management responses are outstanding.

<u>Follow-Up Reviews</u>

Fourteen projects are in the follow-up phase:

- Seven follow-up reviews are in progress.
- Seven follow-up reviews have not been started.

No follow-up review forms are overdue.

Date of Report: January 13, 2026

Report Details

1. **Cybersecurity Audit: Inventory & Control of Operational Technology Assets**
   - Audit scope included all Operational Technology assets supported by the Control Systems Applications Services Team (CSAST) and physically connected to networks maintained by the IOPSS Group as of June 30, 2025.
   - Three (3) recommendations with the following ratings: one **Priority 2**, two **Priority 3**.

2. **First Follow-up Review: Check with Order**
   - Review scope was limited to management's corrective actions resulting from our audit recommendations as of June 30, 2025.
   - Status of four (4) recommendations: one **Implemented**, two **In Process**, one **Closed**.

Other General Auditor Activities

1. Internal Quality Assessment
Preparation for the annual internal quality assessment, as required by professional internal auditing standards, is in progress. Surveys sent to the Board, management, and department staff were received, and we are evaluating and summarizing the results, which will be presented at the March meeting of the Audit Committee.

2. Global Internal Audit Standards
Evaluation and adoption of the updated standards issued by the Institute of Internal Auditors, effective January 9, 2025, are in progress.

3. Audit Manager Position
Collaboration with Human Resources on revising the audit manager job description to complete the department career ladder is in progress.

4. Site Visit
Staff participated in a tour of the Grace F. Napolitano Pure Water Southern California Innovation Center.

5. Training
Staff attended training on P-card, expense report, and time fraud detection.

Office of the General Auditor

Cybersecurity Audit: Inventory & Control of Operational Technology Assets

Project Number: 24-32
December 17, 2025

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

PUBLIC INFORMATION

TABLE OF CONTENTS

PUBLIC INFORMATION

Executive Summary

BACKGROUND

The Center for Internet Security (CIS) is a community-driven nonprofit that has developed the CIS Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data. Its mission is "to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats." Organizations can implement the CIS Critical Security Controls (CIS Controls), a set of 18 controls with detailed safeguards, to improve their cybersecurity posture.

The first CIS control is for the inventory and control of enterprise assets and requires organizations to effectively manage all enterprise assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to determine the totality of assets that need to be monitored and protected within the enterprise.

WHAT WE DID

Our audit scope covered all OT hardware assets, including desktops, laptops, network devices, servers, and non-computing/IoT (Internet of Things) devices, that were supported by CSAST and physically connected to networks maintained by the IOPSS Group (IOPSS networks) as of June 30, 2025.

Our audit objective was to determine whether all hardware assets supported by CSAST and connected to the IOPSS networks are actively managed to determine the totality of assets that need to be monitored and protected.

WHAT WE CONCLUDED

[REDACTED]

WHAT WE RECOMMEND

[REDACTED]

Management agreed with our observations and recommendations.

Information has been removed from this Executive Summary as it contains an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and is for distribution or consideration in a closed session and not subject to the California Public Record Act pursuant to Government Code Section 7929.200.

NUMBER OF RECOMMENDATIONS

0	**PRIORITY 1** Response time: Immediate	
1	**PRIORITY 2** Response time: Within 90 days	
2	**PRIORITY 3** Response time: Within 180 days	

PUBLIC INFORMATION

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Date: December 17, 2025

To: Audit Committee

From: Scott Suzuki, CPA, CIA, CISA, CFE, General Auditor

Subject: Cybersecurity Audit: Inventory & Control of Operational Technology Assets (Project Number 24-32)

We have completed a cybersecurity audit of inventory and control of Operational Technology assets for the Integrated Operations Planning & Support Services Technology Group (IOPSS).

Due to the sensitive nature of the critical infrastructure information, details of our observations and recommendations were shared with select members of the Board and management in a separate confidential report not subject to public release.

Supplemental information, including our scope and objectives, is included in Appendix A. Appendix B includes a description of our new recommendation priority rating system.

We appreciate the courtesies and cooperation provided by the IOPSS Group.

The results in this report will be summarized for inclusion in a status report to the Board. If you have any questions regarding our audit, please do not hesitate to contact me directly at 213.217.6528 or Assistant General Auditor Kathryn Andrus at 213.217.7213.

Attachments

cc: Board of Directors
General Manager
General Manager-Designate
General Counsel
Ethics Officer
Office of the General Manager Distribution
Assistant General Managers
External Affairs Distribution
Integrated Operations Planning & Support Services Group Manager
External Auditor

RESULTS

The Recognition, Results Overview, and Observations & Recommendations sections have been removed from this report as they contain an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and are for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.

EVALUATION OF MANAGEMENT'S RESPONSE

Internal Audit considers management's response appropriate to the recommendations.

AUDIT TEAM

Sherman Hung, CISA, Principal Auditor

APPENDIX A: SUPPLEMENTAL INFORMATION

SCOPE & OBJECTIVES

Our audit scope covered all OT hardware assets, including desktops, laptops, network devices, servers, and non-computing/IoT (Internet of Things) devices, that were supported by CSAST and physically connected to networks maintained by the IOPSS Group as of June 30, 2025.

Our audit objective was to determine whether all hardware assets supported by CSAST and connected to IOPSS networks are actively managed to accurately know the totality of assets that need to be monitored and protected.

EXCLUSIONS

Our audit scope did not include: (1) software assets, (2) data, (3) hardware assets maintained by the Information Technology Group, (4) cloud-based servers, nor (5) servers on virtual machines.

PRIOR AUDIT COVERAGE

We completed the following audit with a similar scope: Cybersecurity Audit: Inventory & Control of IT Assets, Project Number 23-31, issued on March 26, 2025.

AUTHORITY

We performed this audit in accordance with the General Auditor's Internal Audit Plan for FY 2024/25 approved by the Board.

PROFESSIONAL INTERNAL AUDIT STANDARDS

Our audit was conducted in conformance with the Global Internal Audit Standards issued by the International Internal Audit Standards Board.

FOLLOW-UP REVIEWS

The Office of the General Auditor has implemented a new follow-up process to ensure management has effectively implemented corrective action related to our recommendations. Management is required to report recommendation implementation status to our office within six months following the issuance of this report, and a first follow-up review will occur shortly thereafter. All audit recommendations are expected to be implemented within a year of this report, and if necessary, a second follow-up review will occur approximately six months after issuance of the first follow-up review report. Any audit recommendations not implemented after the second follow-up review will be shared with the Board/Audit Committee at its next scheduled meeting.

INTERNAL CONTROL SYSTEM

An internal control system is a continuously operating and integrated component of Metropolitan's operations. Internal controls are implemented by the Metropolitan management and seek to provide reasonable (not absolute) assurance that Metropolitan's business objectives will be achieved. However, limitations are inherent in any internal control system, no matter how well designed, implemented, or operated. Because of these limitations, errors or irregularities may occur and may not be detected.

Specific examples of limitations include, but are not limited to, poor judgment, carelessness, management override, or collusion. Accordingly, our audit would not necessarily identify all internal control weaknesses or resultant conditions affecting operations, reporting, or compliance. Additionally, our audit covers a point in time and may not be representative of a future period due to changes within Metropolitan and/or external changes impacting Metropolitan.

METROPOLITAN'S RESPONSIBILITY FOR INTERNAL CONTROL

It is important to note that Metropolitan management is responsible for designing, implementing, and operating a system of internal control. The objectives of internal controls are to provide reasonable assurance as to the reliability and integrity of information; compliance with policies, plans, procedures, laws, and regulations; the safeguarding of assets; the economic and efficient use of resources; and the accomplishment of established goals and objectives. In fulfilling this responsibility, management judgment is required to assess the expected benefits and related costs of internal control policy and procedures and to assess whether those policies and procedures can be expected to achieve Metropolitan's operational, reporting, and compliance objectives.

APPENDIX B: PRIORITY RATING DEFINITIONS

The Office of the General Auditor utilizes a priority rating system to provide management a measure of urgency in addressing the identified conditions and associated risks. We assess the significance of each observation identified during the audit using professional judgment and assign priority ratings to each recommendation using the criteria listed below. Factors taken into consideration in assessing the priority include the likelihood of a negative impact if not addressed, the significance of the potential impact, and how quickly a negative impact could occur.

	PRIORITY		
	1	2	3
Definition	Observation is *serious* enough to warrant *immediate* corrective action. The condition may represent a serious financial, operational, or compliance risk. A priority 1 recommendation may result from a key control(s) being absent, not adequately designed, or not operating effectively.	Observation is of a *significant* nature and warrants *prompt* corrective action. It may represent a moderate financial, operational, or compliance risk. A priority 2 recommendation may result from a process or less critical control(s) not being adequate in design and/or not operating effectively on a consistent basis.	Observation involves an internal control issue or compliance lapse that can be corrected in the *timely* course of normal business. A priority 3 recommendation may result from a process or control that requires enhancement to better support Metropolitan's objectives and manage risk.
Response Time	Immediate	Within 90 Days of report issuance	Within 180 Days of report issuance

APPENDIX C: MANAGEMENT'S RESPONSE

The Management Response has been removed from this report as it contains an assessment of Metropolitan's vulnerability to terrorist attack or other criminal acts intended to disrupt Metropolitan's operation and is for distribution or consideration in a closed session and not subject to the California Public Records Act pursuant to Government Code Section 7929.200.

Office of the General Auditor

First Follow-up Review: Check with Order

Project Number: 20-1031
December 18, 2025

THE METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

TABLE OF CONTENTS

Executive Summary

BACKGROUND

In November 2020, the Office of the General Auditor completed an original audit of the controls on initiating, authorizing, paying, and distributing accounts payable transactions classified as “Check with Order” (CWO). These transactions occur when an employee requests the return of a signed check for manual delivery to the payee or when a vendor asks to pick up their check directly from the treasury operation team. We also evaluated physical controls over access to the vault room and check stock. Finally, we evaluated the review and approval controls for compliance with sound segregation of duties practices.

The original audit report was issued with a less-than-satisfactory rating and four (4) recommendations regarding checks returned to requestors, reliance on checks, treasury vault access controls, and vendor master file maintenance. Management agreed with three (3) of the four (4) recommendations and partially agreed with one (1) of the recommendations.

In January 2024, management notified us that the three (3) agreed-to recommendations had been implemented, and the one (1) partially agreed-to recommendation had no action taken. Based on this, we initiated our follow-up review on the implemented recommendations.

WHAT WE DID

Our review objective and scope were limited to management’s corrective actions resulting from our audit recommendations as of June 30, 2025 (except as noted otherwise) for the three (3) audit recommendations made and accepted in the original audit, Report on Review of Check with Order, Audit No. 20-1031, dated November 30, 2020.

WHAT WE CONCLUDED

Management has implemented one (1) recommendation, two (2) recommendations are in process, and one (1) recommendation has been closed.

RECOMMENDATION STATUS

1	2	0	1
IMPLEMENTED	IN PROCESS	NOT IMPLEMENTED	CLOSED

THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Date: December 18, 2025

To: Audit Committee

From: Scott Suzuki, CPA, CIA, CISA, CFE, General Auditor

Subject: First Follow-up Review: Check with Order
(Project Number 20-1031)

This report presents the results of our first follow-up review of check with order as of June 30, 2025, original Audit No. 20-1031, dated November 30, 2020.

The follow-up review concluded that the Finance & Administration Group implemented one of the four recommendations, vendor master file maintenance. The recommendations regarding checks returned to requestors and treasury vault access are in process. The recommendation regarding reliance on checks has been closed, as management deemed the risk of using electronic transfers (i.e., ACH) greater than that of issuing checks.

During this follow-up review, we noted several ancillary opportunities for improvement, which have been communicated to management and are included under the Results section. We will conduct a second follow-up review approximately six months after the date of this report to review the implementation status of the two (2) remaining recommendations. We will not follow up on ancillary recommendations as part of the follow-up process, but they will be considered for inclusion in a future audit.

We appreciate the courtesies and cooperation provided by the Finance & Administration Group.

If you have any questions regarding our review, please do not hesitate to contact me directly at 213.217.6528 or Assistant General Auditor Kathryn Andrus at 213.217.7213.

Attachments

cc: Board of Directors
General Manager
General Manager-Designate
General Counsel
Ethics Officer
Office of the General Manager Distribution
Assistant General Managers
Finance & Administration Group Distribution
External Auditor

RESULTS

RECOMMENDATIONS & CURRENT STATUS

1 Checks Returned to Requestors

Checks to be hand-delivered should be returned to an individual other than the requestor.

Recommendation 1

Signed checks should be mailed directly to the payees. In circumstances where mailing is not feasible, someone other than the requestor, preferably a third-party service, should make the delivery. We recommend that the Chief Financial Officer and the Chief Administrative Officer work together to develop policies and procedures to reduce the utilization of checks with orders.

Returning signed checks (negotiable instruments) to the requestor increases the risk that those checks might be altered or delivered to an unauthorized party, placing unnecessary risk on Metropolitan and its employees.

Current Status

In Process.

On February 18, 2021, a district-wide memo was distributed by the Chief Financial Officer and Chief Administrative Officer implementing a revised process for requesting and handling Checks with Orders (CWOs), which took effect on March 1, 2021. The main policy enhancements were:

- Section Manager approval must be obtained (regardless of dollar value).
- Group Manager and Finance approval must be obtained when the check is returned to the requestor (regardless of dollar value).
- Requestor must include a note to the Buyer affirming that the vendor was contacted and will not accept a credit card (P-Card) or standard payment terms (Net 30 days).
- Requestor is to include a note to the Approver that provides a business justification explaining why a CWO is needed for payment.
- Urgent requests shall be labeled as urgent and indicated as such in the applicable iProcurement field.

First, we compared the utilization of checks requested for return during the original audit with those issued during our follow-up review, with the scope of each review covering one calendar year of activity. We noted a 93% decrease from 1,070 checks to 72 checks.

Second, we selected 15 checks requested for return issued between January 1 and December 31, 2023, and reviewed them against current policy.

We performed testing, including both those processed through the requisition process and those submitted directly to accounts payable for processing, and noted three (20%) checks were returned to requestors contrary to the new policy. Upon further review, we noted that these three checks returned to the requestor were for payments that did not utilize the requisition process.

<u>Ancillary Opportunity for Improvement 1</u>

During our review of the 15 checks requested for return issued between January 1 and December 31, 2023 and selected for testing, we also noted:

(1) Ten (67%) requests did not include a note to the Buyer that the Vendor will not accept P-Card or Standard Payment Terms (Net 30 days).

(2) Ten (67%) requests did not include a note to the Approver that provides a business justification explaining why a check requested for return was needed for payment.

(3) One (7%) check requested for return, with a change in the person picking up the check, did not have an email documenting the change. Additionally, this requirement was not included in the updated policy.

We recommend management:

(1) Incorporate into the revised process:

   a. The procedure for returning checks for payments not utilizing the requisition process.

   b. The email notification process to inform Treasury of changes to the person authorized to pick up the check requested for return.

(2) Ensure the person picking up the check is independent of the check request process.

(3) Provide training on the revised process to ensure all those involved in the requesting, processing, and receipt of requested checks returned understand the requirements and their responsibilities.

(4) Conduct periodic reviews to ensure adherence to the revised process and procedures.

2 Reliance on Checks

Organizations should use payment processes that reduce opportunities for fraud by leveraging electronic payments.

Recommendation 2

We noted Metropolitan's ongoing dependence upon printing accounts payable checks. Shifting to payment via Automated Clearing House (ACH) decreases the risk associated with altered or misappropriated checks. Additionally, ACH payments lower transaction costs, are operationally more efficient, and are environmentally friendly.

Reliance on printed checks increases the exposure to altered, counterfeit, or misappropriated checks, potentially resulting in financial loss.

Current Status

Closed.

Management partially agreed with the recommendation. Management determined that increasing ACH transactions is not viable at this time due to the lack of commercially available account validation tools and the increasing cyber risk associated with processing payments electronically. As management has assumed the risk of issuing checks over our recommendation of using electronic transfers (i.e., ACH), we consider this recommendation closed.

3 Treasury Vault Access

Staff duties and responsibilities should define the physical and logical vault access granted.

Recommendation 3

We recommend that the CFO organization maintain authority over access to the vault, evaluate physical access controls, and reconcile these settings against staff duties and responsibilities. We also recommend that management perform periodic access reviews. We understand that management has begun reviewing these procedures.

Failure to maintain access controls could result in unauthorized access to confidential financial systems.

Current Status

In Process.

Treasury has not assumed ultimate approval over all access to the vault. Treasury performed a review ancillary to a system upgrade in 2022 and indicated informal reviews had occurred annually. No further documented reviews could be provided.

Based on management's actions, we consider this recommendation still in process. Treasury should assume access control authority over the vault and should formalize reviews over all those with vault access to ensure that their duties and responsibilities necessitate access. To align the frequency of access reviews with best practice, Treasury should conduct the reviews more frequently than annually (e.g., semiannually).

<u>Ancillary Opportunity for Improvement 2</u>

During our review of the vault room access list, we noted an executive leader was granted access to the vault room due to their oversight of the Treasury function.

This presents a potential segregation of duties conflict, given the breadth of the executive leader's responsibilities in overseeing multiple interconnected functional areas. Access should be based on the principle of least privilege, which is to grant access to the fewest number of individuals and only at the level necessary to allow for the effective execution of an individual's job responsibilities.

We recommend removing the vault room access for the executive leader. If management deems the access as appropriate, we recommend implementing mitigating controls that allow for the timely monitoring of those accessing the vault.

4 Vendor Master File Maintenance

Adequately controlled, the master file ensures properly segregated duties, use of authorized vendors, accurate cash disbursements, and proper tax reporting.

Recommendation 4
We recommend management update the vendor master file and conduct periodic reviews.

Incomplete or outdated vendor records could result in erroneous payments and inaccurate or incomplete reporting.

Current Status
Implemented.

Per the Purchasing System Procedures for Updating Vendors or Suppliers in Oracle, the vendor master file is updated annually by inactivating vendors with no transactional activity within the last three years. Administrative Services Management provided Inactive Vendor Reports for 2021, 2022, and 2023, supporting the performance of periodic reviews. We compared Active Vendors as of January 2020 and March 2024, and noted that the number of vendors without a tax ID decreased by 74%, the number of active vendors decreased by 30%, and the number of vendors with missing addresses decreased by 29%.

Based on the actions taken by management, we consider this recommendation implemented.

AUDIT TEAM

Kathryn Andrus, CPA, CIA, Assistant General Auditor
Chris Gutierrez, CPA, CIA, Program Manager - Audit
Lina Tan, Principal Auditor

APPENDIX A: IMPLEMENTATION STATUS DEFINITIONS

Professional internal auditing standards require internal auditors to confirm that management has implemented internal audit recommendations. The Office of the General Auditor has established follow-up reviews as part of its service portfolio to assess the implementation status of each recommendation from original audits.

Management is required to report recommendation implementation status to our office within six months following the issuance of the original audit report, and a first follow-up review will occur shortly thereafter. All audit recommendations are expected to be implemented within one year of the original audit report. If necessary, a second follow-up review will occur approximately six months after issuing the first follow-up review report. Any audit recommendations not implemented after the second follow-up review will be shared with the Board/Audit Committee at its next meeting.

To facilitate our follow-up reviews, we developed a classification system that rates actions taken by management to implement our recommendations.

IMPLEMENTATION STATUS	
IMPLEMENTED	Management has fully implemented our recommendation, as verified by the follow-up review. No further follow-up is to occur.
IN PROCESS	Management has partially implemented our recommendation. Additional follow-up will occur upon implementation of the remaining actions.
NOT IMPLEMENTED	Management has yet to take action to implement our recommendation. Additional follow-up to occur.
CLOSED	The recommendation has not been implemented, and no further follow-up review will occur due to one of the following conditions: 1. Alternative Action Taken: Management took corrective action that differed from our recommendation. The corrective action sufficiently mitigates the risks associated with the recommendation. 2. No Longer Applicable: Circumstances have changed, and the observation/recommendation is no longer applicable. 3. Risk Assumed: Management has accepted the risk of not implementing or partially implementing our recommendation. The Board of Directors has been apprised of the status. 4. Other: Current status was discussed with the Board, and while our recommendation has been partially implemented, the Board requested no additional follow-up review.