Risk and Audit Committee

Agenda Item 5b

November 17, 2026

Item Name: Review of Independent Auditor's Management Letter

Program: Audit Services

Item Type: Action

Recommendation

Approve the CalPERS Board of Administration's (Board) Independent Financial Statement Auditor's (Independent Auditor) Management Letter for the fiscal year ended June 30, 2026.

Executive Summary

The draft Management Letter, prepared by the Board's Independent Auditor, Plante + Moran, CPAs, includes comments and recommendations related to strengthening internal controls over financial reporting based on the audit of the June 30, 2026, financial statements. Management's concurrence, response, and proposed corrective actions to the observations and recommendations are included in the draft Management Letter. In addition, management reported that the prior year observation was resolved.

Strategic Plan

This item is not a specific product of the strategic plan. Government Code section 20228 requires the board to annually employ a certified public accountant, who is not in public employment, to audit the financial statements.

Background

Plante + Moran, CPAs completed its audit of CalPERS Basic Financial Statements for the fiscal year ended June 30, 2026, as required by Government Code section 20228. In connection with the audit of the financial statements, Plante + Moran, CPAs prepared a draft Management Letter that includes comments and recommendations to enhance internal controls over financial reporting (Attachment 1).

The Management Letter is considered a draft until it is approved by the board and subsequently signed by Plante + Moran, CPAs. The signed Management Letter will be distributed to the board, executive team, and senior management.

Analysis

Consistent with the Office of Audit Services Audit Resolution Policy, the status of the Management Letter observations will be reported to the Risk and Audit Committee until management has resolved each noted observation. The table below summarizes current year observations and the status of the prior year observation.

Table 1 – Status of Current Year Observations -

Observation	Description
1	During our review of user access controls for My CalPERS, we noted that documented user access reviews were not completed by all designated business process owners. This condition was also identified during the prior-year audit. Without complete and documented periodic access reviews, inappropriate, unnecessary, or excessive user access may not be identified and removed timely. Management acknowledges the control deficiency identified regarding myCalPERS user access reviews not being completed by all designated business process owners. We agree that timely and documented periodic access reviews are a critical internal control to ensure that user access remains appropriate, necessary, and aligned with job responsibilities. Management recognizes the significance of this deficiency and the associated risk that inappropriate, unnecessary, or excessive access may not be identified and removed in a timely manner. Going forward, management will establish a documented access review procedure that defines review responsibilities, required documentation, review frequency, and escalation procedures for overdue reviews. Management will also monitor completion of access reviews on an ongoing basis to help ensure that reviews are performed by all designated business process owners and that any inappropriate access is promptly addressed.

Observation	Description
2	During our review of privileged access to AREIS, we identified two user accounts that were granted elevated database administrator access for troubleshooting purposes. The elevated access was not removed following completion of the troubleshooting activities. Additionally, a formal monitoring or review process was not in place to provide oversight of activities performed using privileged access. Privileged accounts provide users with elevated capabilities that may allow significant changes to systems or data. When temporary privileged access is not removed timely and privileged activities are not independently monitored or reviewed, there is an increased risk that unauthorized or inappropriate changes could occur and remain undetected. Management acknowledges the control deficiency identified regarding privileged access to AREIS. We agree that elevated access should be granted only for a defined business need, removed immediately after the need ends, and subject to independent monitoring and review. Upon notification of the issue, management reviewed the two user accounts identified and confirmed they were non-human service accounts that had been granted elevated database administrator access during an outage/troubleshooting event and that the elevated access was not removed when the troubleshooting activity was completed. Management immediately removed the elevated access and confirmed that no other accounts had unauthorized privileged access and that no individuals had access to the credentials for these accounts. Going forward, management will implement a formal process for approving, tracking, and reviewing privileged access to AREIS. This process will require documented approval for temporary privileged access, timely removal of access when no longer needed, and periodic independent review of privileged activity. Management will also assign responsibility for monitoring privileged access to ensure ongoing compliance and to reduce the risk of unauthorized or inappropriate changes going undetected.

Observation	Description
3	During our review of the AVS change management process, we noted that testing was performed for system changes; however, evidence demonstrating the testing performed and results obtained was not formally documented and retained as part of the change record. Without sufficient documentation of testing activities and results, management may be unable to demonstrate that system changes were adequately tested prior to approval and migration to production. Additionally, insufficient testing documentation reduces the audit trail supporting the change management process. Management acknowledges the control deficiency identified regarding the AVS change management process and the absence of formally documented evidence of testing performed and results obtained as part of the change record. Management agrees that documenting testing activities is essential to demonstrate that system changes have been appropriately tested prior to approval and migration to production. Management recognizes the significance of this deficiency and the associated risk that insufficient documentation may impair the audit trail and limit the ability to demonstrate that changes were adequately tested. Going forward, management will require that testing evidence, test results, and related approvals be formally documented and retained as part of the change record prior to production migration. Management will also establish oversight to confirm that required documentation is complete before changes are approved and implemented.

Observation	Description
4	Based on the access information reviewed, one user appears to have privileges that permit both development activities and deployment of changes to the AVS production environment. Allowing a single individual to both develop and migrate changes to production without an effective compensating control reduces segregation of duties within the change management process. This increases the risk that unauthorized, inappropriate, or insufficiently tested changes could be introduced into the production environment without independent detection or approval. Management acknowledges the control deficiency identified regarding segregation of duties within the AVS change management process. Management recognizes that allowing a single individual to perform both development and production deployment activities without effective compensating controls creates a risk that unauthorized, inappropriate, or insufficiently tested changes could be introduced into the production environment. Upon notification, management immediately removed the conflicting access from the affected user, ensuring that no individual currently holds both development and deployment privileges for AVS. Management also performed a lookback review and determined that no changes were migrated to production by this user. In addition, management completed a review of AVS user access rights and confirmed that no other users have conflicting roles within the production environment. Going forward, management will strengthen controls over the AVS change management process by performing periodic user access reviews and independent reviews of AVS users and roles to identify and promptly remediate any segregation of duties conflicts. These reviews will be performed by individuals independent of the development and approval processes to ensure objectivity, and any identified conflicts will be escalated and resolved promptly.

Table 2 – Status of Prior Year Observation -

Observation	Description	Status
1	BDO observed that an approver of changes to be released to production had inappropriate access to the developer role of the Automated Real Estate Investment System (AREIS). The development access allowed this user to develop code modifications to AREIS. We observed a user had the developer role access which grants the ability to develop logic or code and then access to approve/commit this code for release to production. This results in a segregation of duties conflict because it provides the individual with the potential ability to modify the report logic without a secondary approval. Although CalPERS has segregated developers and deployers on the application level, having access to the development and be an approver could bypass Azure DevOps system functionality, which results in a segregation of duties conflict. Additionally, no audit is being performed of the system change log nor database log-in access report to check for and investigate anomalies. CalPERS does have a configuration that requires code changes to be approved by a second user that was observed to be set to require the second approver, but there was no audit log to prove that this configuration was not changed during the audit period. Management has removed the developer access from the user who had inappropriate access to the development environment. To strengthen the change management control environment, it is recommended that the change logs be reviewed on a regular basis for appropriateness by an individual who does not have approver access to AREIS.	Resolved

Budget and Fiscal Impacts

The independent financial statement auditor agreement is from March 1, 2026, to February 29, 2028, for a total amount of $7,408,985. The fee schedule for the basic financial statements audit for the fiscal year ending 6/30/2026 is $1,620,980[1]. Funding was already identified within budgetary resources and is consistent with the board-approved contract.

Benefits and Risks

The primary benefit of approving the draft Management Letter is to assist CalPERS in meeting its fiduciary responsibilities to plan participants by ensuring the effectiveness of controls over financial reporting designed to prevent or timely detect errors that could result in material misstatements in the financial statements. The risk of not implementing recommendations is limiting the timely detection, prevention, or correction of material misstatements in the financial statements.

[1] This amount does not include the $540,500 fee for GASB 68 audits and $187,905 for GASB 75 audits.

Attachments

Attachment 1 – Management Letter (including CalPERS management's responses), prepared by BDO for the fiscal year ended June 30, 2026

Michele L. Nix
Chief Financial Officer
Financial Office

Beliz Chappuie
Chief Auditor
Office of Audit Services

Marcie Frost
Chief Executive Officer