Memorandum

To: Audit Committee of the ISO Board of Governors

From: Ryan Seghesio, Chief Financial Officer & Treasurer

Date: December 12, 2012

Re: **Briefing on Issuance of 2012 SSAE 16 Audit and Scope of 2013 SSAE 16 Audit**

This memorandum does not require Committee action.

EXECUTIVE SUMMARY

On December 13, 2012, the California Independent System Operator Corporation will issue its *SSAE 16 Type 2 Audit* (SSAE 16) for the period from November 1, 2011 to September 30, 2012 and provide the same to the ISO Board of Governors, Management and market participants. The SSAE 16 audit assures market participants the ISO has sufficient internal controls over the processes and procedures of market participant charges and credits, which account for market and congestion revenue rights charges and credits, grid management charges, Federal Energy Regulatory Commission fees, transmission access charges and refunds, and reliability must-run billings.

The auditor's opinion essentially states that the internal control structure is effectively designed to provide adequate controls and that, based on their testing, the controls are in fact operating as designed. Although 2 exceptions were noted, they were determined to be mitigated by other control activities and had no impact on the effectiveness of the controls. Therefore, the control environment was operating effectively during the period.

BACKGROUND

The term *SSAE 16* derives from the auditing profession's Statement on Standards for Attestation Engagements No. 16, *Reports on the Processing of Transactions by Service Organizations*. The ISO is defined as a service organization with respect to our market participants, as market participants utilize the financial information produced by the ISO market billing systems in their own financial systems. In the SSAE 16, independent auditor PricewaterhouseCoopers audits the effectiveness of the ISO bid-to-bill process internal controls. Many ISO market participants have shares that trade on major exchanges governed by the Securities and Exchange Commission. They are subject to the *Sarbanes-Oxley Act*, which requires them to certify the sufficiency of their own internal controls. The SSAE 16 allows them to comply with these reporting requirements for participating in the ISO market.

The ISO's SSAE 16 report follows the standard reporting structure for internal control reports. The report contains an assertion by management that the control environment is effectively designed

and it operated effectively during the period. The report also contains a description of the high-level organizational control environment and a structured presentation of each of our key internal control activities that are organized around 12 control objectives. There are 63 key control activities supporting the control objectives which contain the auditors testing and their results. An exception in an activity can be noted by an auditor and, if not otherwise mitigated by other control activities, can lead to a qualification of the control objective.

Although exceptions were noted for two control activities, they were determined to be mitigated by other control activities and had no impact on the effectiveness of the controls. The exceptions were in activities under two different control objectives.

The first control objective with an exception in one of its activities was control objective 11, which states that controls provide reasonable assurance that changes to the production environment are documented, tested and authorized. There are seven different control activities that support this objective.

The control activity with an exception was control activity 11.7 which is that a system exists and is utilized to monitor changes made to production systems and for identifying and resolving differences between approved and non-approved versions. Exception conditions were identified with respect to this control activity. Four out of twenty-four servers relevant to this control activity were not configured to be monitored by the Tripwire tool for approximately three months of the examination period.

Three other control activities mitigate this activity:

- Control Activity 11.2: Change requests for the production environment are requested and approved for implementation in accordance with approved procedures. This is a preventative control in place to prevent the promotion of changes to the production environment that have not been tested, reviewed and approved by the appropriate manager.
- Control Activity 11.4: Emergency changes to the production environment are reviewed and authorized by IT Management prior to implementation. This is a preventative control in place to prevent emergency changes from being made to the production environment that have not been authorized by IT management.
- Control Activity 11.6: Prior to implementation into production, all requests for deployment are approved by the cross-functional change advisory board and assessed for work package completeness. This is a preventative control that prevents planned production changes from being promoted to production without appropriate review and approval by the change advisory board.

These control activities which mitigate the exception conditions were tested without exception and, thus, the report concluded that the control objective was achieved.

The second control objective with an exception in one of its activities was control objective 12, which states that controls provide reasonable assurance that the process of maintaining physical and logical security minimizes the risk of unauthorized access to, use of, modification of, damage to, or loss of, IT facilities or information. There are 16 different control activities that support this objective.

The activity with an exception was control activity 12.13, which is that on an annual basis, privileged access to systems is reviewed and reaffirmed by Management to determine that access rights remain commensurate with job responsibilities and proper segregation of duties is maintained. Exception conditions were identified with respect to this control activity In connection with the annual assessment of privileged users. Action was not taken in accordance with established procedure to address 10 privileged user accounts that were identified as requiring further investigation to determine if their access rights were appropriate.

Two other control activities mitigate this activity. They were:

- Control Activity 12.9: Procedures are in place for provisioning internal user logical access to ISO information systems and services. This is a preventative control in place to control the provisioning of all new user access to the network, database, and operating systems.
- Control Activity 12.11: Procedures are in place for de-provisioning internal user logical access to ISO information systems and services in accordance with ISO policy. This is a preventative control in place to provide for the removal of access for users that are terminated or whom no longer require access to the network, database and operating systems.

These control activities which mitigate the exception conditions were tested without exception and, thus, the report concluded that the control objective was achieved.

The SSAE 16 is a comprehensive report covering our control environment. It does, however, exclude certain activities that are not subject to this control structure, such as the quality of meter data received from the market or the control room decision making processes.

The ISO control environment reflects the overall viewpoint, awareness, commitment and actions of the Board, Management, and market participants. Management constantly reviews activities underlying the bid-to-bill process for improvement opportunities, with process improvement as one of our top priorities.