CalPERS

Legal Office

Memorandum

November 4, 2019

To: Members,
Risk and Audit Committee

From: Matthew G. Jacobs
General Counsel

Subject: Process for Designating Information in Internal Audit Reports as Confidential

Introduction

At the September 2019 Risk and Audit Committee meeting, the Committee asked management to report back with "an overview of our current practices as it relates to the confidentiality of [internal] audit reports, to review best practices for organizations in the maintenance of confidentiality of reports, current law, and to provide staff's recommendations for changes, if any, to our current practices." (Transcript of 9/17/19 RAC Meeting, p. 5.) This is the requested report.

Best Practices and California Law

With respect to industry best practices, the standards internal auditors use is the Institute of Internal Auditors' (IIA's) International Standards for the Professional Practice of Internal Auditing (Standards) (2017). The IIA is the internal audit profession's most widely recognized provider of standards, guidance, and certifications. In fact, California law requires State internal auditors to conduct their audits under the standards prescribed by the IIA. See Cal. Gov't Code section 13886.5(a) ("The Controller, the Director of Finance, and the respective staffs thereof, and all state agencies that have their own internal auditors or that conduct internal audits or internal audit activities, shall conduct internal audit activity under the general and specified standards of internal auditing prescribed by the Institute of Internal Auditors or the Government Auditing Standards issued by the Comptroller General of the United States, as appropriate.").

The "Disseminating Results" section of the Standards, section 2440, requires an organization's chief auditor to communicate the results of an audit "to [internal] parties who can ensure that the results are given due consideration." Standards, section 2440.A1, p. 19, available at https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf.

As for external parties, the Standards caution auditors to be careful:

> If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the [Chief Auditor] must:
>
> - Assess the potential risk to the organization.
> - Consult with senior management and/or legal counsel as appropriate.
> - Control dissemination by restricting the use of the results.

Id., § 2440.A2.

The IIA's International Professional Practices Framework (Framework) (2019) elaborates on the IIA's Standards. With respect to the "Disseminating Results" standard, the Framework explains:

> To ensure compliance with legal obligations and organizational protocols, it is important for the [Chief Auditor] to take great care and consideration when preparing to disseminate results outside of the organization. In addition, the [Chief Auditor] should consider the ramifications of communicating sensitive information, as such information might impact the organization's market value, reputation, earnings, or competitiveness. The [Chief Auditor] may find it helpful to consult with legal counsel and compliance areas within the organization.

Framework, Implementation Guide 2440 – Disseminating Results, p. 189.

In addition to this general directive to internal auditors to mind the sensitivity of audit reports in considering whether they can be disseminated to third parties, California law specifically protects some internal audit reports from disclosure, either in whole or in part. Specific exemptions are provided for in the Public Records Act (PRA) and more generally in the Evidence Code and the Government Code, among others.

<u>CalPERS' Current Practices</u>

CalPERS' practices conform to both industry best practices and California law. As the Board is aware, internal audits are undertaken to examine the enterprise's risk management, control, and governance processes. At CalPERS, no operational area, no matter how sensitive, is exempt from audit. Moreover, auditors do not know at the outset where an audit will lead, what it will find, or how sensitive it will be.

CalPERS' auditors from the Office of Audit Services (OFAS) summarize the results of these examinations in audit reports that are then provided to management and Board members. As explained in the "Issuance of Audit Report" section of OFAS's "Audit Process" document:

> Once we [OFAS] receive the Executive management's response to the draft report, we finalize the report. We include the audit response into the report and include the signed cover memo as an appendix to the report. The report is addressed to the Chief Executive Officer via the General Counsel. We send copies to responsible division management, members of the Risk & Audit Committee,

and specified Executive management. At this point, the audit process is complete and the audited division can begin follow-up and resolution efforts.

See OFAS, Audit Liaison Guide, Appendix III: Audit Process (July 2013), p. A-12.
(Although this procedure says that OFAS distributes the audit reports to the RAC, in practice OFAS distributes them to all Board members.)

These audit reports may contain proprietary, market-sensitive, and other confidential information that could harm CalPERS' investments, investment strategy, physical or digital security, and/or litigation posture if disclosed publicly. Because OFAS consults with the Legal Office on developing its audit plan, on legal issues that arise during audits, and on final determinations regarding confidentiality and exemptions from disclosure based upon the above, once OFAS completes an audit report, management initially designates the report as attorney-client privileged and attorney work product to preserve the confidentiality of the report while the Legal Office completes its analysis.

Specifically, the Legal Office reviews it and assesses whether any privilege or exemption continues to apply to it. If we determine that no privilege or exemption applies to any part of the report, the report will not be considered confidential. If we determine that only parts of the reports are confidential, those parts will be designated accordingly.

Whether or not a report or a part of a report is deemed confidential informs the way CalPERS handles the report internally and how it responds to a request for the report, under the PRA or otherwise. Upon receipt of a PRA or other third-party request for an internal audit report, CalPERS' PRA Unit can respond by producing the report, producing the report with redactions, or by declining to produce the report, depending on the Legal Office's prior analysis. For example, the audit of CalPERS' Network Security Management (IA17-016) contains sensitive information about CalPERS' IT security infrastructure that hackers could exploit if it were available to them. Based on the Legal Office's review, CalPERS would decline to produce that internal audit report in response to a PRA request, citing Government Code section 6254.19, which exempts certain IT security information from disclosure. Conversely, we recently received a PRA for several internal audits of Investment Office processes. After the Legal Office reviewed the requested reports, CalPERS produced them to the requestor with minor redactions.

Conclusion

CalPERS' practices with respect to designating information in internal audit reports as confidential comports with industry best practices and California law. Therefore, management is not recommending any changes to them. Of course, if the Board has any additional questions about these processes, we would be happy to answer them.

cc: All Board members and Designees