January 14, 2020

Mark Ghaly, Secretary
California Health and Human Services Agency
1600 9th Street #460
Sacramento, CA 95814

Dear Dr. Mark Ghaly,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the Office of Systems Integration submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2019.

Should you have any questions please contact Bob Huskison, Chief Administrative Officer, at (916) 263-1709, bob.huskison@osi.ca.gov.

GOVERNANCE

Mission and Strategic Plan

The Office of Systems Integration's (OSI's) mission is to procure, manage, and deliver technology systems that support the delivery of health and human services to Californians. Since its inception, the OSI has developed a track record of successfully managing and deploying large, complex, mission critical systems to support health and human services programs at the state, federal, and local levels. The 2019-2024 Strategic Plan (updated July 2019) is in place and available on the department's Intranet site, accessible to all OSI staff. The plan outlines the OSI's strategic organizational objectives and goals, such as adopting a culture of collaboration and innovation, focusing on outcomes and value generation, using data to drive action, and expanding project portfolios.

Control Environment

OSI executive management has established an effective control environment by implementing policies, guidelines, and procedures that reflect and safeguard the values of the organization. The control environment encompasses both technical competence and ethical commitment. The establishment, communication, and reinforcement of these policies, guidelines, and procedures form the basis of an effective control environment in that OSI management and employees:

- Understand their responsibilities; the limits of their authority; and are knowledgeable, mindful, and committed to doing what is right and doing it the right way
- Pledge to following the organization's policies and procedures, and its ethical and behavioral standards

To provide guidance and assistance to OSI management, a current strategic plan and mission statement are in place. Further, appropriate controls and governance are in place to monitor and review operations and programs. Regarding the authorization and approval of transactions, financial policies and procedures are in place and communicated to all applicable employees. In response to departures from approved policies and procedures, or violations of the code of conduct, OSI management takes appropriate disciplinary action.

OSI's organizational structure is clearly defined and up to date, with the appropriate reporting relationships established and communicated to all employees. Current job descriptions that detail the responsibilities and qualifications for each position are recorded and maintained. In order to help ensure control procedures are followed and resources are used efficiently, qualified personnel are hired and provided relevant, ongoing training.

Information and Communication

The OSI currently uses a departmental communication plan for conveying information both vertically and horizontally across organizational lines to achieve departmental objectives.

Staff have the opportunity to communicate both internally and externally in the following meetings:

- Leadership Meetings - Includes the Directorate, Chief Counsel, Agency Information Officer, and Deputy Directors. Occurs monthly.
- Executive Staff Meetings - Includes the Leadership Team, Project Directors, and Administration Division Chiefs. Occurs monthly.
- Project Status Meetings - Includes individual project management (including Deputy Director) and Directorate. Occurs monthly.
- Division Meetings - Deputy Directors hold division meetings with staff. Occurs either monthly or quarterly.
- Regular staff meetings at the project and unit level – Includes all OSI state staff. Fixed agenda with questions and answers. Occurs biannually.
- Standing Project Governance meetings - Includes project staff, and leadership from OSI, project sponsors, and stakeholders. Project governance is the main vehicle for identifying project risks and issues and is highlighted in greater detail in this report under Risk number one. Occurs on a regularly scheduled basis.
- Project Review Board meetings - Includes project staff, leadership from CHHSA, OSI, and project sponsors. These Board meetings also serve to highlight specific risks, issues, and challenges with IT projects within the OSI portfolio. Occurs regularly.

The organization uses SharePoint and the Intranet as the prime repositories for operational, programmatic, and financial information.

MONITORING

The information included here discusses the entity-wide, continuous process to ensure internal control systems are working as intended. The role of the executive monitoring sponsor includes facilitating and verifying that the Office of Systems Integration monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to:
Bob Huskison, Chief Administrative Officer.

As a project management organization, the OSI is continually identifying risks and issues and addressing vulnerabilities. The OSI currently leverages a departmental communication plan for monitoring the internal system of controls. Monitoring opportunities consist of the following meetings:

Leadership Meetings, Executive Staff Meetings, Project Status Meetings, and Division Meetings. In addition, there are standing Project Governance meetings and regularly occurring Project Review Board meetings, which serve to highlight specific risks, issues, and challenges with IT projects within the OSI portfolio. These meetings are outlined in greater detail in the Information and Communication section.

The OSI has implemented ongoing monitoring processes as outlined in the monitoring requirements of California Government Code sections 13400-13407. These processes include reviews, evaluations, and improvements to the OSI systems of controls and monitoring.

Using this formal reporting information, as well as other informal data, the Chief Administrative Officer and Chief Deputy Director regularly review and discuss the effectiveness of internal controls. Any changes that are required are decided upon and immediately implemented.

RISK ASSESSMENT PROCESS

The following personnel were involved in the Office of Systems Integration risk assessment process: executive management, middle management, and front line management.

The following methods were used to identify risks: brainstorming meetings, ongoing monitoring activities, audit/review results, other/prior risk assessments, external stakeholders, questionnaires, consideration of potential fraud, and performance metrics.

The following criteria were used to rank risks: likelihood of occurrence, potential impact to mission/goals/objectives, timing of potential event, potential impact of remediation efforts, and tolerance level for the type of risk.

The OSI uses the departmental communication plan and the previously mentioned communication opportunities to identify risks. Discussions regarding risks and issues are regularly discussed at these meetings and items are identified that could lead to reduced project functionality, increased cost, project delays, and, in the worst case, failures in project delivery. These include risks and issues within both the projects and administrative areas. Items that cannot be identified adequately and addressed at the lowest level are escalated to executive management for discussion and prioritization.

Risk ranking is accomplished through discussion at the Leadership and/or executive level. Prioritization is considered by gauging the impact of risks and issues across the organization, both in severity and breadth. Risks and issues that stand to impact all parts of the organization or are of such an impact that they could severely impact smaller parts of the organization, are measured, discussed, and decided upon.

RISKS AND CONTROLS

Risk: Difficulty Retaining and Recruiting Staff

The OSI faces difficulty training, retaining, and recruiting staff needed to carry out the specialized nature of certain project work and program expertise due to roles requiring specialized skillsets. Retirement and turnover also contribute to the loss of knowledge in the workforce, and OSI struggles to find replacement staff with the technical knowledge and qualifications to develop and maintain the organization’s large and complex projects.

The OSI is not able to carry out its mission effectively when critical positions remain unfilled. Failures and delays in project delivery are potential risks that can result from the inability to recruit qualified staff.

Control: A

- Establish a Workforce Development Plan for recruiting, developing, and retaining an experienced, highly technical, and strong workforce
- Utilize social media platforms to recruit and retain talent

Control: B

In addition to the Workforce Development Plan, the OSI is working to:

- Ensure guidelines and manuals are updated or developed for all projects/divisions processes
- Pilot a manager/supervisor rotation program
- Cross-train staff on mission-critical processes
- Utilize knowledge transfer tools to document business processes and procedures for leadership and critical positions

Risk: Insufficient Structure for Security Processes

There is a lack of standardized security processes across the organization. As a result, the department may be more vulnerable to cyberattack and possible loss of critical protected health information (PHI) and Health Insurance Portability and Accountability Act (HIPAA) data due to inconsistent security policies and lack of established security standards.

Control: A

In May 2019 the OSI hired an Information Security Officer. Since that time the Information Security Office (ISO) has become fully staffed and has had primary focus on the following areas:

- All information security policies are being updated and aligned to NIST800-53 standards, and will be reviewed on a bi-annual basis
- OSI completed the California Military Department Independent Security Assessment in November 2019, and we are actively working to mitigate the findings
- ISO staff are monitoring, securing and auditing the internal network on a daily basis with existing and new technologies in order to meet the security requirements of protecting our network and data

Control: B

In 2020 the OSI will continue to make progress in the above areas, in addition, the OSI Information Security Office will:

- Review all new project contracts pertaining to information security to ensure that the appropriate level NIST 800-53 security control requirements are specified for monitoring, auditing and overall security architecture, and for data security and privacy
- Collaborate with the OSI programs to develop and document procedures in compliance

with the new security policies
- Commission an outside vendor for a Tier 1 - “Organization level” risk assessment of the entire OSI information and technology environments

Risk: Lack of Resources to Respond to Program Changes

The OSI identifies the inability to respond timely to address changes in Program Requirements from Federal and State Levels due to insufficient resources as a risk. Although there is a dynamic nature to most projects at the OSI, the constantly changing regulations and policies that affect our projects are difficult to meet because of lack of resources, time, or funding.

This impacts project delivery as limited resources are being redirected to handle program and policy changes.

Control: A

- Collaboration between OSI, project sponsors, stakeholders, and control agencies allow for resources to be redirected, where available and appropriate, to ensure that these changes can be addressed.
- Modification of existing project plans and resources, such as personnel and budget, is also utilized to address program and policy changes that must be implemented.

Risk: Inadequate and Inefficient Data Reporting Practice

There are no practices in place to ensure that data is collected consistently and reported in a timely manner. Additionally, duplicative reporting requirements result in an inefficient use of enterprise resources.

Control: A

- Through the evaluation of current cost reporting practices and the resulting implementation of standardized project cost reporting, ensuring consistency of cost categories, methodologies, and the way the data is collected, the risk of inconsistent data collection is mitigated.
- The use of tools such as Microsoft SharePoint and Power BI currently provide for, and in the near future will expand, the organization’s ability to provide replicable reporting functionalities across disparate project types resulting in reporting that is not duplicative and resulting staff skill sets that are transferrable across the various project efforts within the organization.

CONCLUSION

The Office of Systems Integration strives to reduce the risks inherent in our work and accepts the responsibility to continuously improve by addressing newly recognized risks and revising risk mitigation strategies as appropriate. I certify our internal control and monitoring systems are adequate to identify and address current and potential risks facing the organization.

Dan Kalamaras, Director

CC: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director of California Department of Finance
Secretary of California Government Operations Agency