December 19, 2019

Julie Lee, Acting Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Ms. Julie Lee,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the California Department of Tax and Fee Administration 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 Katie Hagen, Chief Deputy Director , at (916) 324-4490, Katie.Hagen@cdtfa.ca.gov.

GOVERNANCE

Mission and Strategic Plan

The California Department of Tax and Fee Administration (CDTFA) administers California's sales and use, fuel, tobacco, alcohol, and cannabis taxes, as well as a variety of other taxes and fees that fund specific state programs. CDTFA-administered programs collect over $70 billion annually to support local essential services such as transportation, public safety and health, libraries, schools, social services, and natural resource management programs.

CDTFA’s Mission, Goals, and Objectives are as follows:

Mission: We make life better for Californians by fairly and efficiently collecting the revenue that supports our essential public services.

Goal 1: Modernize Tax Collections to Adapt to the 21st Century Economy

A. Streamline processes and harness state-of-the-art technologies (i.e., Centralized Revenue Opportunity System) to enhance tax collection, improve accuracy, boost efficiency, and speed tax administration.

B. Adapt to meet the challenges of a changing economy, including online sales, cannabis legalization, and point of sale technologies.

C. Create a culture of continuous improvement with proper internal controls.

D. Use data to assess staffing levels, organizational structure, and performance measures.

Goal 2: Improve Taxpayer Services

A. Expand online service for taxpayers.

B. Increase outreach, communication, and education efforts.

C. Minimize taxpayer burden and increase compliance.

Goal 3: Support Our Team

A. Improve recruitment, selection, and onboarding to ensure team members have the skills necessary to carry out our mission.

B. Create a workplace culture where all team members feel valued, and are able to contribute their full talents.

C. Develop CDTFA team members by providing high-impact training, valued mentoring, and knowledge transfer – all essential to succession planning.

D. Promote and sustain an ethical workplace culture.

CDTFA has over 75 business plan initiatives in support of these goals and objectives. Our current Strategic Plan can be found on our website at www.cdtfa.ca.gov.

Control Environment

CDTFA's management is committed to honesty, integrity and ethical behavior. These values are central to CDTFA's control environment. Ethical concerns are reported through our Employee Hotline, the State Whistleblower hotline, and the Director's Comment Box.

Oversight is provided by the Director. CDTFA Senior Staff, which consists of the Director, Chief Deputy Director, Deputy Directors, and various Bureau Chiefs, exercises appropriate levels of responsibility and authority over their program areas to establish an effective control environment.

CDTFA has adopted the 'Three Lines of Defense' model, as outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This model allows the department to establish and coordinate duties related to risk and control. The model proposes that the Enterprise Risk Management Committee (ERMC) oversee and direct three lines of defense that contribute to effective management of risk and control.

These three lines consist of the following:

1st line of defense--Operational Management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks. This includes recruiting, developing, and maintaining a competent workforce; as well as, evaluating performance and enforcing accountability.

2nd line of defense--ERMC, Information Technology, Governance and other control functions monitor and facilitate the implementation of effective risk management and assist the risk owners in reporting adequate risk related information throughout the department.

3rd line of defense--Internal Audit Bureau, through a risk-based approach to its work, provides assurance to the department's audit committee and Senior Staff that internal control systems are in place and documented. This assurance covers the effectiveness of the 1st and 2nd lines of defense.

Information and Communication

Senior Staff meets weekly to discuss operational and programmatic issues within the organization.

These meetings are used to collect and communicate relevant information needed for decision making purposes. In some cases, work groups are created. These work groups report back to Senior Staff on various operational, programmatic, and financial decision making. Additionally, the Director and Chief Deputy Director meet with Deputy Directors in one-on-one meetings on a regular basis.

The CDTFA uses several channels to communicate with team members across the enterprise:

- Senior Staff members share information with their managers and supervisors at their respective staff meetings.
- CDTFA Director conducts frequent Town Hall meetings that are live streamed throughout the department and team members participate by asking questions in person or via email.
- External Affairs Division (EAD) prepares the CDTFA *Express*, a weekly electronic newsletter.
- EAD created an Intranet site (*i*CDTFA) to facilitate communication.
- Internal campaigns utilizing posters, banners and emails.
- Program areas conduct Town Halls for training (i.e., processing contracts, hiring process, etc.).
- Human Resources Bureau conducts New Employee Orientation.
- Administration Division conducts an employee engagement survey.

Channels for communicating and sharing information with external stakeholders include:

- CDTFA website
- Special Notices
- Newsletters
- Social Media
- Tax and fee payer workshops and seminars
- Interested Parties Meetings
- Annual Taxpayer Bill of Rights meetings
- Open Data Portal
- Meetings with control agencies

CDTFA team members are able to report inefficiencies and inappropriate actions to management using the following methods:

- Managers and Supervisors' meetings with their team members.
- Director's Comment Box, which can be found on *i*CDTFA intranet, allows team members to submit suggestions, feedback, and comments to the Director.
- Employee Hotline allows all team members—rank and file, supervisory, management—to report employee misconduct confidentially and without fear of reprisal. The Internal Affairs Section (IAS) investigates complaints and allegations involving violations of policies or laws relating to CDTFA employees.
- Diversity and Inclusion Office handles concerns regarding sexual harassment, discrimination based on age (over 40), race, sex, (including pregnancy, childbirth, breastfeeding, or related medical conditions), ancestry, color, religion, disability (physical or mental), national origin, marital status, political affiliation, sexual orientation, gender identity, gender expression, medical condition, and military and veteran status; or retaliation related to an EEO complaint.
- State Auditor Whistleblower Program allows team members to report on employee misconduct and improper activities to the State Auditor; an annual email on the program is sent to all team members.

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 California Department of Tax and Fee Administration monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to: Nicolas Maduros, Director; and Katie Hagen, Chief Deputy Director .

CDTFA has established an ERMC. CDTFA's Director is the chair of the ERMC and Senior Staff are a part of the governing body. The ERMC takes a risk-based approach to managing the department's risks and integrating concepts of internal control and strategic planning. The ERMC team conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the department. CDTFA takes measures to successfully reduce risks and vulnerabilities to a reasonable and appropriate level.

In addition, the Financial Management Division meets weekly to methodically work through complicated legacy audit findings and prepares a quarterly dashboard of enterprise-wide performance metrics to spot anomalies and enhance efficiency.

External auditors, CDTFA Internal Audit Bureau, and CDTFA Information Security Office also identify and address vulnerabilities by ensuring policies, procedures, standards and/or guidelines are effective. These vulnerabilities are monitored through reports and Corrective Action Plans (CAPs).

RISK ASSESSMENT PROCESS

The following personnel were involved in the California Department of Tax and Fee Administration risk assessment process: executive management, middle management, front line management, and staff.

The following methods were used to identify risks: brainstorming meetings, employee engagement surveys, 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.

RISKS AND CONTROLS

Risk: Team Member Safety

Because CDTFA is a tax collection agency, team member safety is at greater risk when performing compliance, collection, audit, and enforcement activities, which could result in physical threats and/or harm.

Control: A Field Office Controls

CDTFA is implementing a Safety Assessment schedule for field offices to ensure that each office is reviewed every 2 years by Business Management Bureau team members and every 4 years by CA Highway Patrol.

In addition to these assessments, the Field Operations Division (FOD) will mitigate risk to team members and the public by internally performing an on-going assessment of individual field offices and implementing appropriate security measures. These efforts combined are designed to improve overall safety and ensure a more secure environment in which to interact with the public.

The assessments will help CDTFA maintain secure facilities that are up to date with security trends and improved technology. After the assessments are completed, recommendations will be implemented according to ease of implementation and financial viability. Those items deemed urgent or emergent will receive immediate consideration and be submitted to the Director and Chief Deputy Director for approval.

Control: B Headquarters Controls

CDTFA is implementing a Safety Assessment schedule for Sacramento area offices to ensure that each office is reviewed every 2 years by Business Management Bureau (BMB) team members and every 4 years by California Highway Patrol. In addition to these assessments, BMB team members will mitigate risk by implementing and updating security measures and educating team members on safety procedures. These efforts combined are designed to improve safety and ensure a more secure environment.

Control: C Enforcement Activity Controls

The CDTFA Investigations Division's (ID) efforts to ensure the safety of ID team members enforcing compliance evolves due to new and changing industry/business practices. Through training and working with law enforcement, team members will be safer. Team member safety will improve through more training and working with law enforcement. This will be an ongoing effort.

Control: D Department-wide Controls

CDTFA will improve policies and procedures surrounding badging. BMB is working to improve the badge design that would be implemented according to badging policy. CDTFA will also implement a new temporary badging system for visitors; update and improve policies and procedures; adopt a standard that is in line with our mission, vision and goals, and improve the accuracy and timing of allowing visitors into the secure area. BMB is working to determine the best software solution based on market research and the experience of other state agencies. Both activities will help prevent unauthorized access to CDTFA buildings.

Risk: Data Security

The security of confidential, as well as Personally Identifiable Information (PII) and other sensitive data, is critical to CDTFA's ongoing mission. A breach of confidential data within the CDTFA Infrastructure, including the Centralized Revenue Opportunity System (CROS) and statewide Financial Information System for California (FI$Cal), may lead to the department's inability to effectively administer California taxes and fees, revenue loss, and damage to CDTFA's reputation. Internal and external acts threaten the confidentiality and privacy of CDTFA information assets.

CDTFA utilizes the NIST Cybersecurity Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. Consequently, the following security controls follow the structure of the Framework. Described at a high-level, these controls (*functions*) and sub-controls (*categories*) are performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risk.

Control: A NIST Cybersecurity Framework- Identify

Identify—An essential part of data security is the identification of assets, enterprise governance, and regular risk assessment. CDTFA must ensure:

- Hardware and software is inventoried according to applicable standards
- Organizational communication and data flows are mapped for compliance
- Priorities for organizational mission, objectives, and activities are established and communicated
- Dependencies and critical functions for delivery of critical services are established
- Organizational cybersecurity policies and procedures are established
- Cyber threat intelligence is received from information sharing forums and sources
- Threats, vulnerabilities, likelihoods, and impacts are identified and used to determine risk

For an organization, the first step in mitigating risk is through identification (i.e., of assets, processes, etc.). Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts consistent with its risk management program and business needs.

Control: B NIST Cybersecurity Framework- Protect

CDTFA develops and implements appropriate safeguards to ensure critical services are delivered. These safeguards adhere to state and federal mandates (e.g., SAM 5300, NIST SP 800-53, IRS P1075, etc.). The following sub-controls enable CDTFA to protect its information assets:

- Logical, physical, and remote access is managed, as well as access permissions (to apply principles of least privilege and separation of duties)
- CDTFA users are informed and trained—additionally, privileged users and physical and cybersecurity personnel understand their roles and responsibilities
- Data-at-rest and in-transit is protected through implementation of the latest available technologies and standards
- Development and testing environments are separate from production environments
- Baseline configurations for CDTFA systems are created and maintained on a regular basis
- Configuration change control processes are in place
- Data is destroyed according to policy and procedure—IRS Publication 1075 standards

Proper protection controls help limit or contain the impact of a potential cybersecurity event. Moreover, these measures entail constant and continual analysis and revision—providing the organization with real-time data for improving its security posture.

Control: C NIST Cybersecurity Framework- Detect

Detect—CDTFA has developed and implemented activities to identify the occurrence of cybersecurity events. Without detection capabilities, the confidentiality, integrity, and availability of an organization's information assets are entirely vulnerable. To combat this situation, CDTFA has implemented the following sub-controls:

- Event data are collected and correlated from multiple sources and sensors
- Incident alert thresholds are established
- The network is monitored to detect potential cybersecurity events
- Personnel activity is monitored to detect potential cybersecurity events
- Monitoring for unauthorized personnel, connections, devices, and software is performed
- Vulnerability scans are performed on a regular basis

Event detection information is communicated, and detection processes are continuously improved.

Proper detection capabilities enable timely discovery of cybersecurity events, as well as total prevention in some cases. The effective implementation of these controls also lends itself to response and recovery activities in cases of a cybersecurity event.

Control: D NIST Cybersecurity Framework- Respond and Recover

CDTFA has implemented response and recovery activities in the event that its data is compromised in a detected cybersecurity event. These activities maintain resilience and restore any capabilities or services that were impaired due an incident. CDTFA must ensure:

- Response and recovery plans are executed during or after an incident (e.g., annual delivery of the following documents: Business Impact Analysis (BIA), Business Resumption Plan (BRP), and Technology Recovery Plan (TRP))
- Personnel know their roles and order of operations when response and recovery is needed
- Incidents are reported consistent with established criteria
- Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources
- Newly identified vulnerabilities are mitigated or documented as accepted risks

CDTFA response activities support its ability to contain the impact of a potential cybersecurity incident. Recovery activities support timely recovery to normal operations to reduce the impact from a cybersecurity incident. When incorporating lessons learned from both sets of activities, CDTFA is better prepared to secure its data in the future.

Risk: Key Person Dependence and Succession Planning

The lack of a published succession plan and recruitment strategy, as well as under-optimized hiring and onboarding processes, contribute to poor employee retention. The loss of institutional knowledge from preventable attrition and elongated hiring processes is a severe risk to the organization.

Control: A Implement a Robust Workforce Plan

CDTFA plans to mitigate the risk by:

- Implementing the CDTFA Succession Plan,

- Establishing cyclical policy attestations to align with the reporting cycle of mandatory trainings,
- Streamlining and automating the hiring process to ensure appropriate and timely filling of vacancies,
- Creating a consistent and customized Onboarding process for all new hires,
- Creating and implementing a Recruitment Strategy including Diversity and Inclusion initiatives,
- Continuing employee retention and enrichment initiatives,
- Proactively reviewing and updating organizational structure to enhance oversight and division of labor, and
- Organizing mentoring and developmental opportunities to cultivate the department's next generation of leaders.

These control activities will assist in retaining institutional knowledge from preventable attrition and elongated hiring process and will make CDTFA into a destination employer.

Risk: Internal Control Systems

The lack of internal controls systems may result in the inability of the CDTFA to meet its fiduciary responsibilities to accurately and effectively manage state resources.

Control: A Ensure Policies and Procedures are Current

Policies continue to be revised and posted to the CDTFA intranet site (*i*CDTFA).

- Programs (i.e., Human Resources, Business Management, Technology Services, Financial Management, Diversity and Inclusion) continue to assess and transition their policies from BOE-Board related standards and practices to those required for CDTFA's Manual of Administrative Policies (CMAP).
- The CMAP Coordinator will begin work with programs to maintain a policy matrix that identifies the status of Board of Equalization Administrative Manual (BEAM) policies (i.e., transferred to CMAP, in progress, sunset).

The CMAP Coordinator will work with Programs to monitor "Revision Date" updates to ensure the polices remain current.

Keeping policies and procedures current and up-to-date reduces risk by providing accountable persons with the tools needed to accurately and effectively perform their roles and responsibilities in compliance with current statutory provisions.

Control: B Implement Business Practices and a System of Internal Controls

CDTFA will implement business practices and a system of internal controls to accurately and efficiently manage resources. Focusing on best business practices and strong internal controls reduces risk by creating an organizational culture and structure that sets standards to ensure proper segregation of duties, reconciliations, reviews and approvals, along with reporting and monitoring responsibilities. These types of controls significantly limit theft, loss, misuse and misappropriation and encourages a work environment focused on constant improvement.

Given changes to the CDTFA and Financial Management Division, the CDTFA team has developed new procedures, including Retail Sales Tax Fund allocation and bank reconciliation procedures. In addition, the Financial Management Division has engaged an external accounting consultant to assist in a) resolving longstanding and significant audit issues that date back to 2014, and b) implementing best practices of comparable tax departments in other states.

CDTFA team members will further refine procedures as the department's IT systems stabilize and business processes evolve. Partner with accounting consultant to fully address remaining audit issues and implement best business practices.

Control: C Integrate Internal Controls with IT Systems such as CROS and FI$Cal

CDTFA will integrate internal controls with the department's IT systems, Centralized Revenue Opportunity System (CROS) and FI$Cal as well as leverage performance metrics and analytic dashboards to enhance business operations.

In partnership with FI$Cal, SCO, DOF, and CROS, the Department is a) developing an interface between CROS and FI$Cal, and b) exploring opportunities to streamline its revenue remittance process. In 2019, CDTFA launched enterprise-wide performance metrics and is now tracking performance against newly established targets.

CDTFA will a) continue working with FI$Cal, SCO, DOF, and CROS teams to implement an interface between CROS and FI$Cal; b) explore opportunities to enhance our revenue remittance process; and c) will monitor its performance metrics against internal targets.

CONCLUSION

The California Department of Tax and Fee Administration 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.

Nicolas Maduros, 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