December 29, 2023

Joe Stephenshaw, Director
California Department of Finance
915 L Street
Sacramento, CA 95814

Dear Director Joe Stephenshaw,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the California Health Benefit Exchange submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2023.

Should you have any questions please contact Thien Lam, Program Integrity Director, at (916) 228-8600, Thien.Lam@covered.ca.gov.

GOVERNANCE

Mission and Strategic Plan

The California Health Benefit Exchange's (Covered California) mission is to increase the number of insured Californians, improve health care quality, lower costs, and reduce health disparities through an innovative, competitive marketplace that empowers consumers to choose the health plan and providers that give them the best value.

In September of 2023 the Covered California Board formally adopted a three-year strategic plan to guide our organization's decisions, set priorities, establish initiatives, and prepare annual budgets. The Board's adoption of staff's strategic plan reinforced the revised strategic pillars and core values that represent how Covered California will continue to fulfill its mission and deliver on the promise of providing Californians with access to high-quality, affordable health care. This strategic plan will serve as our roadmap for the next three years, enabling us to make significant strides in our initiatives and continuously improve our services for the benefit of our consumers.

Covered California's six strategic pillars and underlying strategic goals:

Affordable Choices: We connect consumers to financial assistance and a choice of affordable plans and providers that give them the best value.

Strategic Goals:

- Connect as many Californians as possible to financial assistance to maximize take-up of affordable coverage.
- Ensure that all Californians have robust and meaningful choices and understand their choices of affordable coverage.
- Research, implement improvements, and provide technical assistance to inform the policy dialogue about lowering premiums and out-of-pocket costs for consumers.

- Participate in and reinforce the state's efforts to contain costs.

Quality Care: We ensure consumers consistently receive accessible, equitable, high-quality care.

Strategic Goals:

- Produce measurable, equitable improvements in health outcomes.
- Hold qualified health plan and qualified dental plan issuers accountable for consistent, standard levels of quality.
- Increase access to and support of high quality, diverse providers who practice with cultural humility.
- Make demonstrable progress in addressing health disparities and increasing health equity.
- Increase access to and quality of behavioral health care.

Organizational Excellence: We foster a nimble culture of continuous improvement that empowers and motivates our team to deliver on our mission with high standards.

Strategic Goals:

- Attract, retain, and invest in our team by fostering an inclusive, innovative, and collaborative workplace culture.
- Maintain and enhance Covered California's trusted brand and reputation through transparency, accountability, security, and sustainability.
- Optimize data as meaningful information to drive decision making.
- Incorporate diversity, equity, and inclusion in everything we do.
- Provide employees with the tools, training, and support they need to do their jobs well.

Reaching Californians: We are unwavering in our pursuit to reach Californians and connect them to comprehensive and affordable coverage.

Strategic Goals:

- Reach all Californians, including those most in need of coverage through a culturally resonant and linguistically appropriate, data-driven approach.
- Strive to enroll and maintain coverage for as many Californians as possible.
- Develop a comprehensive community engagement strategy to enhance our ability to reach historically marginalized communities and populations statewide.
- Utilize data and technology to customize outreach, facilitate enrollment, and minimize gaps in coverage for Californians.
- Expand efforts to connect California's small business owners and their employees to affordable coverage, either through Covered California for Small Business (CCSB) or the individual marketplace.

Catalyst for Change: We pioneer new ideas and disseminate our learnings to drive improvement in health care in California and nationally.

Strategic Goals:

- Build and use evidence to empower decision makers and foster innovation in how to deliver affordable coverage and quality care.
- Enhance the way we share the innovative work that Covered California is doing.
- Increase alignment between and amplify the work of partners, including Medi-Cal, the California Public Employees' Retirement System, the California Department of Health Care Access and Information, and the California Department of Managed Health Care to enhance affordability, coverage, quality, and equity.

Exceptional Service: We provide the highest level of service and exceed our consumers' expectations.

Strategic Goals:

- Provide consumers with a seamless and consistent consumer experience regardless of which channel they use.
- Make the self-service enrollment process as simple as possible and provide a seamless transition to assistance when needed.
- Provide clear and understandable information to assist consumers to apply for, use and maintain coverage, in a culturally resonant and linguistically appropriate way.
- Increase the consistency and efficiency of consumer interactions with Covered California and enrollment partners.

As Covered California looks to the future and builds upon the Affordable Care Act (ACA), our strategic plan strives to improve our workplace, our marketplace, our health care system, and our state. Our commitment to diversity, equity, and inclusion runs across all six pillars as the lens we apply across our work. Across the six pillars, our consumers remain our North Star. Four central strategies summarize how we aim to improve our consumers' experiences and outcomes:

- **Coverage You Can't Miss:** We will reach Californians where and when they need us, while ensuring historically marginalized and hard-to-reach populations aren't left behind.
- **Coverage That Resonates:** We will construct our efforts for all Californians, deepening our understanding of the needs of our diverse communities and further tailoring our strategies to meet them.
- **Coverage That's Easy:** We will minimize barriers to coverage by having our system do the work for consumers, rather than consumers having to work for our system.
- **Coverage For California's Future:** We will maximize our levers to achieve hard-fought progress on affordability, cost, quality, and equity.

Our Core Values:

- **We Value People.** We respect people for who they are and value their contributions. We seek and embrace diverse perspectives. We create an inclusive and welcoming environment for all through behaviors that show empathy and care for others. We empower individual talent to help create positive impacts for consumers, Californians, and their communities.
- **We Work Together**. We create a culture of trust and shared responsibility. We actively

seek opportunities to engage and collaborate with our partners and stakeholders. We are transparent in our decision-making and welcome input.
- **We Do the Right Thing.** We operate with the highest degree of honesty, respect, and fairness in everything we do. We take ownership and responsibility for our decisions and hold ourselves and others accountable. We are mindful stewards of the public trust and responsibly manage our resources.
- **We Innovate.** We value curiosity, responsible risk-taking, and enthusiastic pursuit of new ideas even at the risk of failure. We are nimble and unafraid of change. We foster creativity that challenges constraints and drives progress.
- **We Follow Through.** We keep our commitments and do what we say we will do. We are results-driven and focus on outcomes that will deliver the highest value to Californians.

Covered California's strategic pillars and corresponding goals will guide the organization when making decisions, setting priorities, and preparing annual budgets.

Control Environment

Covered California is governed by a five-member Board. The Executive Office, composed of the Executive Director, Chief Deputy Executive Director of Operations, Chief Deputy Executive Director of Program, Chief Deputy Executive Director of Clinical Operations, and the Chief Deputy Executive Director of Program Compliance and Accountability, develops organizational strategy and provides leadership direction in concert with the Board. The Executive Office provides broad oversight of operations and is tasked with supporting team members as well as a broad community of individuals and groups (including the Board, stakeholders, and the public) with the direction, information, tools, and support they need to achieve our mission. Our control environment is modeled after The Institute of Internal Auditors' Three Lines Model. The first Line is the greatest opportunity to identify risks. All managers are risk managers that monitor and oversee their internal controls imbedded in their day-to-day operations. The second Line includes Enterprise Risk Management, the Information Security Office, and various Compliance units housed within divisions. These areas monitor, provide expertise, support, and assist with related risk matters in concert with the divisions to support the Executive Office and Senior Leadership. The third Line includes the Office of Audit Services, which provides independent and objective assurance and advisory services to help the divisions reach their goals by testing procedures and providing recommendations to remediate control gaps. This third Line helps assure the Executive Office, Senior Leadership, and the Board that internal controls are in place, working as intended, and are effective. Each Line works collaboratively on the control environment and risk assurance towards the effective and efficient operations of Covered California and reports relevant risks to the Executive Office and Board.

Covered California embodies integrity and ethical values through its governance structure and processes, which include the Board's and the Executive Office's oversight. Leadership takes to heart the mission, vision, strategic plan, and core values of the organization. One of our core values is "We Do the Right Thing": Covered California works to earn the public's trust through its commitment to accountability, responsiveness, transparency, speed, agility, reliability, fairness, and cooperation. Leadership demonstrates doing the right thing through integrity and ethics in the work they do and the actions they take. These actions reinforce a

positive tone at the top that is infused throughout the organization. Covered California promotes these values by modeling them, promoting them, and creating a safe and trusting environment in which to work. Managers exemplify and promote ethical behavior. Our culture encourages prompt reporting of unethical behavior. This accountability and action to address concerns reinforces Covered California's commitment to integrity and ethical values. To ensure all Covered California team members and contractors are aware of their responsibility and role in maintaining an ethical workplace, management and all officials must complete the mandated state employee ethics training. Management uses policies and various communication strategies (e.g., emails, memos, newsletters, performance appraisals, and meetings) to communicate the standards of conduct to all team members. Team members at all levels are encouraged to report potential risks. Reporting channels include forms available on the intranet for reporting harassment, discriminatory action or practices, information security incidents, privacy incidents, fraud, and risk or internal control concerns. Along with these forms, team members are encouraged to talk with their supervisors or their human resources liaison if they are unsure how to escalate a particular concern. They can also reach out to each area for assistance via email, phone, or Microsoft Teams.

Documentation of internal control systems is developed and maintained at the organization and division level. Internal controls are communicated to team members through various channels such as written policy and procedures, Covered California University, enterprise-wide communication through task guides, the intranet, emails, and meetings. Documentation is reviewed and updates to the policies and procedures are made as changes in state and federal legislation or regulation occur or as business needs evolve.

In addition, an Enterprise Risk Management infrastructure was developed to foster collaboration across all divisions and share knowledge and resources on sound governance, risk, and compliance management principles and practices. This improves operational performance in order to support Covered California's mission and strategies.

Enterprise Risk Management works to build a risk-intelligent culture by meeting with divisions to discuss current and potential risks, identify gaps or weaknesses in controls, and document internal controls. Enterprise Risk Management holds regularly scheduled risk discussion meetings. These meetings welcome all areas of the organization to attend, share their voice, and participate in the decision-making process. These meetings focus on initiative specific risks that impact the organization. Risks are identified, rated on their impact to the organization, likelihood of occurring, and how well the controls mitigate the risk. The risk and controls are then reassessed as the initiative progresses. The Enterprise Risk Management team also proactively reaches out to divisions to offer training and assistance in identifying and documenting potential risks and control gaps. Enterprise Risk Management engages with risk and control owners to complete risk assessments through our risk collaboration process. Enterprise level risks will be brought to the Risk Alliance forum comprised of all Division Directors or their delegates for assessment. This allows a forum for enterprise-wide risks to be discussed at the leadership level.

The Executive Office meets bi-monthly with Directors to discuss escalated issues (e.g., new legislation, organizational goals, etc.), and any current and emerging risk(s). The Executive Office receives reports which include risk summaries, risk rating criteria, risk assessments, and

mitigation strategies.

All divisions encourage accountability, transparency, effectiveness, efficiency, and risk management by independently reviewing key policies, business areas, and operations to comply with state and federal laws, regulations, and policies. Covered California divisions recognize the importance of compliance and accountability. Examples of program level accountability include the Service Center's Quality Assurance Program; the Policy, Eligibility, and Research Division's Eligibility Compliance Unit, which ensures we comply with policies and regulations; the Regulatory Compliance Unit within the Office of Legal Affairs; and the Data Integrity Section within the Program Integrity Division. In addition to program led accountability, the Enterprise Risk Management Unit works with the divisions to conduct biennial enterprise risk assessments. The enterprise risk assessment enhances accountability and partnerships. The results of the biennial enterprise risk assessment are shared with the Executive Office and Senior Leadership, holding us accountable as an organization.

Information and Communication

Covered California employs many different processes to collect and communicate relevant and reliable information necessary for operational, programmatic, and financial decision making. We are an evidence-based and data-driven organization. The way in which we collect, validate, and reconcile data ensures that it is reliable and in sync when it is transmitted and stored between multiple systems. We collect data through our systems as well as consumer focus groups and surveys. Focus groups and surveys provide invaluable qualitative and quantitative data to tell us where we may need to reconsider, adjust, or create new policies. They also help us discover where we can develop and improve operational efficiencies.

Partnership is a primary value for Covered California, which is reflected in our five core values: We Value People, We Work Together, We Do the Right Thing, We Innovate, and We Follow Through. Partnership efforts are guided by working with consumers, providers, issuers, employers and other purchasers, government partners, and other stakeholders. As mentioned above, we engage with our consumers and collaborate with the Centers for Medicare and Medicaid Services, State Controller's Office, Department of Finance, and Department of General Services. In addition, the Executive Office and Senior Leadership meet regularly with the Board to communicate relevant and reliable information to act on important policies that strive to achieve the organization's mission, core values, and objectives.

We also value the input of many other external partners. The Open Enrollment Kick-Off Meetings are joined by agents, certified enrollers, county partners, elected representatives, and other stakeholders. On a regular basis, Covered California meets with external stakeholders and advocacy groups. Another example of our commitment to partnerships, is our weekly calls to qualified health plan issuers. These calls discuss upcoming changes and priorities so that all parties can ask questions. The goal is to plan accordingly for seamless policy and operational changes that impact the consumer. Additionally, we publish press releases, webinars, and emails to communicate information to external parties.

Relevant and reliable information is communicated to team members through various channels. The Executive Office hosts monthly meetings to share program updates. Unit,

divisional, and project meetings are a normal practice for management and team members to share information on a timely basis. In these meetings, risks may be discussed, documented, and rated. Team members understand the importance of reporting risks. Risks and controls are regularly assessed at initiative meetings and cross-divisionally during the risk discussion meetings.

Covered California shares information in risk discussion meetings to minimize silos and to assess the impact of changes across the organization. These cross-divisional collaborations ensure understanding and program and priority alignment. The Enterprise Risk Management team will also facilitate a Risk Alliance forum to discuss enterprise risks at the Senior Leadership level to ensure all business areas have insight into risks that may impact their area. This forum will allow divisions to be aware of the high-level risks and provide their input into how the risk may impact their business area, what controls they may be able to own to help mitigate the risk, and provide their insight into the impact and likelihood of the risk occurring.

As a part of Covered California's commitment to continuous improvement, we are dedicated to nurturing and advancing our risk culture. Being risk-intelligent is about being aware of the potential challenges we may face, and ensuring we have robust strategies in place to manage them effectively. Our ongoing efforts to enhance our risk management process and provide comprehensive training underline our commitment to fostering a risk-intelligent culture. This commitment is not limited to our risk management team but extends to every one of us.

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 Health Benefit Exchange monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to: Thien Lam, Program Integrity Director.

Covered California requires divisions to maintain internal controls to actively monitor day-to-day operations and identify concerns as they arise. Each division is responsible for documenting and implementing their ongoing monitoring processes as required by the State Leadership Accountability Act. This involves reviews, evaluations, and continuous improvements to the current monitoring processes to identify potential control opportunities. Each division must ensure that their processes comply with internal policies and legal requirements as well as effectively mitigate risk. Divisions monitor their processes to ensure they perform as expected by completing internal compliance reviews and may work with Enterprise Risk Management, which can facilitate discussions to identify potential gaps in the process and help the division develop and implement controls to mitigate any gaps. Covered California's Service Center Quality Assurance Unit embodies our commitment to mitigating risk through effective monitoring processes. This Unit regularly monitors consumer calls to ensure accurate information is provided, monitors training materials to ensure they remain current, and monitors procedures to assess the strength of their controls, along with other monitoring activities. Along with the Office of Legal Affairs, the Policy, Eligibility, and Research Division's Eligibility Compliance Unit monitors relevant legal developments to ensure current processes and procedures comply with rules and regulations. The Carrier Management, Certification,

and Contract Branch is another example of Covered California's commitment to risk mitigation. This Branch ensures that qualified health and dental plan issuers are complying and performing to their contractual obligations. In addition to the divisions' monitoring efforts, Enterprise Risk Management works with the divisions to identify areas of opportunity to strengthen internal controls.

Along with day-to-day monitoring, the Program Integrity Division oversees the establishment and processes for monitoring internal controls and evaluating the results. The division includes five key assurance areas to evaluate and monitor our internal controls: California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS) Testing and Performance Review Section, Data Integrity Section, Integrated Fraud Management Unit, Enterprise Risk Management Unit, and Office of Audit Services.

CalHEERS Testing and Performance Review Section conducts ongoing testing of CalHEERS. CalHEERS is Covered California's real-time online automated eligibility and enrollment system that:

- Serves as the consolidated system support for eligibility, enrollment, and retention for Covered California and Modified Adjusted Gross Income (MAGI) Medi-Cal.
- Streamlines resources from which individuals will be able to research, compare, check their eligibility, and purchase health coverage.

This team conducts ongoing testing of CalHEERS through User Acceptance Testing, Baseline Testing, and Post-Implementation Review to confirm that enhancements and other system changes comply with business rules, design documents, and state and federal regulations. The team also specializes in researching and providing recommendations to internal and external organizations regarding issues identified through testing.

The Data Integrity Section is another area within Program Integrity. They manage, monitor, and reconcile consumer data to verify that the qualified health and dental plan issuers have accurate eligibility and enrollment data. This helps consumers access affordable plans and providers that give them the best value.

The Integrated Fraud Management Unit proactively detects and prevents fraud, waste, and abuse. Its efforts help Covered California comply with applicable state and federal laws and regulations regarding fraud management to combat fraud before it occurs. The Integrated Fraud Management Unit is the central fraud reporting hub for Covered California divisions, external partners, qualified health and dental plan issuers, and stakeholders. When a complaint is brought to our attention, the team performs a thorough assessment which includes reviewing applications and monitoring agent and qualified plan issuer websites to confirm issues are being addressed. The results are shared with our internal and external stakeholders to improve their processes in order to deter fraud, waste, and abuse.

The Enterprise Risk Management Unit provides oversight of risk management to ensure effective integration and coordination of all risk management activities. In addition, they provide the organization with education and services to help identify and assess risks and control activities.

The Enterprise Risk Management Unit maintains a risk database which identifies, documents, prioritizes, and tracks all risks. Risk identification, assessment, and reporting are standard practices throughout the organization. As part of the risk assessment process, Enterprise Risk Management monitors the risks and controls logged in the database. This activity includes conducting internal reviews of the information and discussing the risks and controls with the owners to ensure the risks are properly described, the controls are valid, and the risk rating criteria for each risk are accurate.

The Office of Audit Services is an independent, assurance business area designed to improve our organization's operations and compliance. The Office of Audit Services helps Covered California accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The annual risk-based audit plan is developed with the assistance of information obtained through our biennial risk assessment process.

The identification of potential risks and control concerns occur in several ways. Enterprise Risk Management may reach out to divisions, or vice versa, to discuss a potential risk or internal control concern. Covered California encourages all team members to report a potential concern through the risk reporting form housed on the intranet site or by contacting Enterprise Risk Management directly.

Depending on the concern identified, Enterprise Risk Management works in concert with the divisions to identify and document the risk(s); inform affected divisions of the risk; and identify controls, assess the risk(s), and set up a monitoring plan. If a risk impacts multiple divisions or is an enterprise risk, additional discussion and review with a larger audience will occur.

The Enterprise Risk Management Unit facilitates enterprise-wide risk assessments and spearheads the biennial enterprise risk assessment process in concert with the Executive Office and Senior Leadership. Furthermore, through two-way communication, risk collaboration, and enterprise-wide risk assessments, Enterprise Risk Management collaborates to promote transparency across the organization, cultivate organizational alignment, support resource allocation, and build partnerships. These collaborations break down silos and create an enterprise-wide view of risks and mitigating controls.

Enterprise Risk Management engages with the organization to promote a risk-intelligent culture, prioritize risk(s), and foster transparency. This occurs through the following actions:

- Regularly scheduled risk discussions involving leadership and any interested team members. The risks and controls to major initiatives are discussed in these meetings.
- Risk collaboration meetings focus on a key risk and include the risk and control owners. The group defines the risk, functional objective, risk statement, root causes, current controls, and the necessary controls to mitigate the risk.
- The Risk Alliance will be composed of Division Directors or their delegate and their subject matter experts. Enterprise level risks will be brought to this forum for discussion at the organizational level. Newly identified risks or concerns may be raised at this forum to determine the risk owners and next steps. Risks that have been discussed through the risk collaboration process will also be brought to the forum for additional insight and to determine if all impacted divisions have been properly identified. This forum

promotes transparency and discussion. It allows all divisions to have a voice in sharing their thoughts of how the risk may impact their division and the organization.

Any identified control deficiencies are promptly addressed, with a clear focus on prioritizing, measuring, and monitoring these until fully remediated. Through various channels, we identify and assess control deficiencies. Following identification, the Risk Alliance members, team members, and management collaborate to prioritize these issues based on their potential impact. Our team then measures the effectiveness of the control improvements we implement and closely monitors progress until the risk is mitigated and the control is fully implemented. This diligent approach to control deficiencies ensures our operational effectiveness, compliance with regulatory requirements, and most importantly, the high-quality healthcare service we offer to Californians.

RISK ASSESSMENT PROCESS

The following personnel were involved in the California Health Benefit Exchange 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.

Enterprise Risk Management oversees and monitors Covered California's risk management assessment and reporting process. The risk management process assists all divisions with their risk analysis and evaluation of operations, internal controls, policies, and procedures. As part of the risk reporting process, divisional managers must assess each identified risk. The assessment requires consideration of the impact the risk could potentially have to the organization and its strategic plan; likelihood of the occurrence; and an evaluation of the current internal controls or mitigating strategies. Enterprise risks are tracked and monitored on an ongoing basis. These risks will be reviewed by the Risk Alliance to foster and promote transparency, collaboration, communication, and partnership across all divisions and recommend priorities to the Executive Office.

RISKS AND CONTROLS

Risk: Information Security

At Covered California, we are entrusted with a significant responsibility - the protection and security of confidential data, including personally identifiable information of our consumers. This trust forms the backbone of our relationship with our consumers and partners, and our ability to deliver on our mission. Failure to safeguard this sensitive information could potentially erode this trust and hinder our capacity to provide Californians with access to high-quality

health care. This emphasizes the criticality of data security in our operations and our commitment to uphold it.

Objective: To ensure Covered California has the appropriate controls in place to deliver affordable health care to Californians.

Control: Technical Controls

Covered California is committed to the protection of consumer information and consistently reviews and updates technical controls to ensure they meet current laws and address emerging threats.

Covered California's Information Technology Division (ITD) will ensure multi-factor authentication has been implemented throughout all systems. This will require the user to consistently provide both something they know and something they have to gain access to Covered California's systems. ITD is in the process of improving threat detection and response through an outsourcing agreement to provide 24/7 event log monitoring. This arrangement will free up ITD resources to focus on escalated events and other projects to protect confidential information. ITD is in the final deployment of a leading endpoint detection and response (EDR) solution across all workstations and servers. Using artificial intelligence to analyze behavior, the EDR platform can both detect and block potential threats.

A critical aspect of addressing unauthorized access is to have a robust Identity Access Management program. Based on the principle of least privilege, ITD has implemented comprehensive role-based access procedures for granting access to Covered California systems. ITD has an initiative to enhance this process through automation. Eliminating the manual process of provisioning users will reduce the risk of errors. Automating deprovisioning tasks will allow for a timelier disabling of accounts no longer needed, which will reduce the risk of unauthorized access.

Control: Security Awareness Training and Prevention Tools

Insider threats are a security risk from within, such as Covered California employees and contractors. To tackle these threats, Covered California has been educating its employees about how to stay secure online. This is done through yearly training sessions, monthly tips, internal tests, and reminders. These efforts help employees realize how crucial their role is in maintaining security. In addition, to address insider threats, Covered California has two upcoming technology initiatives for Fiscal Year 2024-2025 to provide additional data protection in the area of access and transmission of sensitive information. These strategic investments underscore our dedication to maintaining the highest standards of data security and ensuring the trust of our consumers and partners. As we advance our technology, we continue to prioritize the protection of confidential data, including personally identifiable information of our consumers.

Control: Inventory Management and Patching

Covered California acknowledges the significance of robust asset management and

timely patching as key strategies to mitigate the risks associated with outdated technology. In pursuit of this, Covered California's ITD is in the process of deploying an advanced asset management solution designed to enhance the accuracy of the technology inventory. This improved inventory will strengthen the risk management capabilities and ensure better compliance by providing a comprehensive understanding of our assets, their associated vulnerabilities, and the required security controls.

Additionally, ITD is spearheading an initiative aimed at enhancing the overall patching program. Patching allows for the application of security updates. The main objective is to achieve consistency and timeliness in the application of system security updates. By streamlining the patching process, ITD will improve the overall security posture of the Information Technology (IT) environment.

Control: Compliance Management

Covered California is committed to complying with all relevant state and federal legislation. Failure to implement updated laws could potentially impact Covered California's security posture, operations, and reputation. The Center for Medicare and Medicaid Services (CMS) governs the information security program related to the CalHEERS IT environment, which is compliant with the current CMS framework, Minimum Acceptable Risk Safeguards for Exchanges (MARS-E). CMS will require all Health Benefit Exchanges to comply with the MARS-E replacement, Acceptable Risk Controls for ACA, Medicaid, and Partner Entities, by early 2025. In addition, Covered California is subject to two new CA laws, AB 749 (State Agencies: Information Security: Uniform Standards) and AB 2135 (Information Security). These laws impact the information security program requiring additional security controls throughout both CalHEERS and Covered California IT environments. Following the current compliance management procedures, Covered California IT and the Information Security Office will implement the new security requirements with ongoing monitoring with an expected completion by the end of 2024.

Control: Outsourcing and Employee Development

In today's competitive market for technology talent, Covered California has been challenged with hiring and retaining qualified information security professionals. To meet the demands of maintaining a robust information security program, Covered California maintains partnerships with technology firms to provide highly skilled technical professionals to support the Information Security Office. Using full-time and project-based outside resources has allowed the Chief Information Security Officer to move forward with concurrent initiatives. In addition, Covered California is committed to taking care of employees and provides existing technical employees with training for continued growth and development.

Risk: New and Changing Legislation (State and Federal)

Failure to implement new and changing legislation could jeopardize Covered California's financial position, potentially impact our operations and reputation, and impede our efforts to serve our consumers. Recognizing this, we put a strong emphasis on understanding, adapting

to, and implementing legislative changes swiftly and efficiently.

Objective: To ensure Covered California successfully implements new and changing legislation in a timely manner.

Control: Change Control and Governance Process Over CalHEERS

To implement new legislation and operationalize changes, Covered California creates and prioritizes placeholder system Change Requests. This allows CalHEERS to reserve resources needed to implement changes to ensure timely compliance. CalHEERS Change Control and Governance Process, comprised of Covered California, Department of Health Care Services (DHCS), and CalHEERS, initiates, reviews, and approves all changes that affect the system. A change management system controls the lifecycle of all changes, minimizes disruptions to the production system and records and maintains change approvals. Security impacts are analyzed prior to the Change Advisory Board's (CAB) final review. Major system changes require a Change Notification submission to CMS followed by written CMS approval. Proposed changes are fully tested to validate desired outcomes and ensure security and quality. Upon successful testing, CAB reviews the production change then sets schedules to reduce operation impacts. Change execution is validated to ensure system integrity and security. Business areas further validate testing before system release. Updates to Change Requests include record of final implementation, maintained within the change management system.

Control: Legislation Analysis, Tracking, Monitoring, and Feedback provided to Regulatory Agencies, Congress, and Legislature

Covered California has a dedicated team that works with impacted divisions that tracks and analyzes proposed state and federal legislation, regulations, and executive orders throughout the year. In addition, Covered California also tracks and analyzes administrative guidance, which is often issued during an administration change. Monitoring these legal and policy developments allows Covered California to formulate implementation strategies and identify potential impediments well in advance of needing to make such changes. Covered California also offers comments to proposed regulations during public comment periods and provides technical assistance to the state legislature and Congress on proposed legislation. Feedback to regulatory agencies, Congress, and the legislature allows Covered California to articulate how proposed legislation or rules impact Covered California and potentially resolve operational barriers before such changes are finalized.

Control: Internal and External Stakeholders Collaboration, and Implementation Workgroups for Impacted Divisions

Covered California coordinates with both internal and external stakeholders to identify challenges with implementing proposed legal and policy changes. Covered California convenes internal workgroups with impacted divisions to discuss implementation challenges; timelines to achieve compliance; and possible technical assistance or public comment to address issues. Covered California also consults with its external partners,

including advocates, issuers, state and federal agencies, state exchanges, and enrollment partners. These external communications allow Covered California to gather feedback on how proposed legislation or regulations affect its external partners who are integral to fulfilling Covered California's mission and, most importantly, its consumers.

Control: Gather Feedback, Inform Internal and External Partners, and Participate in Joint Application Design Sessions to Support Changes in Interfacing Partner Systems

Covered California works with the Office of Technology and Solutions Integration and DHCS to address competing priorities, evaluate impacts to interfacing partner systems, and discuss possible technical assistance. Covered California coordinates with both internal and external stakeholders to inform them of upcoming policy and system changes, especially those with expedited timeframes. Covered California also participates in regular meetings with DHCS, Statewide Automated Welfare Systems (SAWS), California Welfare Directors Association (CWDA), the Center for Consumers Information and Insurance Oversight, and qualified health and dental plan issuers to inform all parties of changes and ensure alignment on priorities. These meetings allow Covered California to gather feedback before system design on how upcoming system changes will affect external partners who play a vital role in fulfilling Covered California's mission and, most importantly, serving its consumers. Additionally, Covered California participates in Joint Application Design (JAD) sessions hosted by CalHEERS to ensure system design meets the needs of all partner state agencies and interfacing systems.

Control: Internal and External Workgroups to Address System Consumer Experience Challenges Due to Different Programs Between Covered California and Medi-Cal

Covered California coordinates with stakeholders such as DHCS, SAWS, CWDA, advocates, state exchanges, certified enrollers, and qualified health and dental plan issuers to inform them of upcoming policy and system changes. Our goal is to evaluate program differences when applying for Insurance Affordability Programs to reduce consumer burden, gather feedback, and develop innovative solutions with all stakeholders and consumers.

Covered California participates in the JAD sessions and the Human Centered Design sessions hosted by CalHEERS to confirm that the system design reduces or eliminates consumer experience challenges and addresses the needs of all partner agencies and interfacing systems. CalHEERS is designed to dynamically present application questions based on a preliminary program-level evaluation to enhance the consumer journey when applying for Covered California or Medi-Cal through the CalHEERS Single Streamlined Application program. Covered California provides education through various channels to consumers regarding the differences between Covered California and Medi-Cal programs to alleviate consumer confusion as they apply for Insurance Affordability Programs.

Risk: Workforce Succession Planning, Key Person Dependence

Without a sufficient, standardized knowledge transfer process to ensure adequate continuity of business processes, Covered California may be subject to loss of knowledge and experience if key persons leave the organization due to attrition. Additionally, inadequate succession planning and ineffective recruitment and retention strategies may result in increased turnover and vacancy rates for key positions critical to Covered California's mission, jeopardizing organizational resilience and long-term success.

Objective: To ensure Covered California maintains the critical knowledge and information necessary to sustain core business processes, advance strategic initiatives, and effectively execute workforce succession planning.

Control: Knowledge Transfer Tools

The absence of adequate knowledge management tools and effective knowledge transfer practices poses a risk to the organization, potentially leading to a loss of critical institutional knowledge, hindering innovation, and impeding organizational agility. Preserving institutional knowledge is crucial when employees move on from their roles in the organization through transfer or separation. Covered California is working to develop and implement a comprehensive knowledge transfer system that includes user-friendly tools such as hosting a SharePoint site and developing templates for division's use to facilitate efficient transfer among employees, ensuring critical information is documented, accessible, and consistently updated.

Control: Consultation/Assessment for Leadership Development Training

To successfully prepare the next generation of high-level leaders within Covered California, the organization must build a culture where mid-level managers and supervisors feel confident and motivated to take the next step in their careers. To create competent, forward-thinking leaders within the organization, Covered California will provide managers and executives with the opportunity to participate in advanced leadership development programs as well as provide training needs assessment and consultations when needed. Covered California will work to expand the availability of these services to increase their accessibility to emerging leaders within the organization.

Control: Exit Survey and Turnover Trend Analysis and Reporting

By developing, implementing, and continuously assessing a comprehensive exit survey process, coupled with ongoing turnover trend analysis, Covered California may systematically gather feedback from departing employees to identify recurring patterns and proactively address root causes of turnover. Learning why employees are leaving the organization will provide insight to refine retention strategies and identify opportunities for improvement within management. This control enables the organization to gain insights into employee perceptions, pinpoint areas for improvement, implement targeted retention strategies, and foster a more supportive and engaging work environment to mitigate the risk of high employee turnover.

Control: Career Advancement Opportunity Awareness

Covered California is developing and implementing a comprehensive in-house career services program that offers employees access to personalized career counseling sessions, guidance on identifying and preparing for professional development opportunities, and assistance in creating personalized career paths within the organization. This program will give employees an awareness of what career advancement is available to them, based on their current eligibility or long-term career goals, in the organization and state service overall. This control aims to enhance employee retention, satisfaction, and engagement, by demonstrating a commitment to their long-term career success in state service. By providing an accessible career planning resource, Covered California aims to reduce the risk of high turnover through increased job fulfillment and the perception of a supportive and growth-oriented work environment.

Risk: Third-Party Contractor Risk

There is a risk that Covered California may be negatively impacted by our third-party contractors, caused by ineffective data security and privacy controls, compliance issues, inconsistent quality of service-level agreements, and poor performance that may damage Covered California's reputation. This may result in contractual disputes, non-compliance with regulations, financial issues and unexpected costs, and operational and service interruptions.

Objective: Establish a comprehensive contract and risk management framework that identifies, assesses, and addresses potential vulnerabilities associated with our third-party contractors. This includes refining our existing contracting processes, negotiating contractual terms that clearly define obligations and responsibilities, and instituting ongoing monitoring to proactively identify and mitigate risks throughout the contract lifecycle. The overarching goal is to enhance the organization's resilience against third-party risks, safeguarding Covered California's interests, reputation, and financial well-being.

Control: Third-Party Risk Management Program

As part of the ongoing effort to manage enterprise risk, the Information Security Office (ISO) in partnership with the Business Services Branch (BSB) and the Office of Legal Affairs (OLA) is tasked with implementing and maintaining a comprehensive third-party risk management program. This program is designed to mitigate the risks associated with third-party contractors.

ISO will develop risk classifications based on the contracted services, criticality to Covered California, and the type of information shared. For example, third-party contractors that access and store consumer personal information are deemed a higher risk classification than a third-party contractor that is not involved with consumer data. ISO, BSB, and OLA will revise our existing privacy and security contract addenda to apply them based on risk classifications. Third-party contractors will be contractually obligated to adhere to privacy and security safeguards appropriate for the potential risks to Covered California and for the protection of the data entrusted to them.

Comprehensive risk-based pre-contract security assessments will be incorporated into the

process which will bolster our ability to preempt and mitigate potential risks posed by third-party contractors. In addition, third-party contractors will undergo ongoing monitoring through annual assessments where they will be expected to furnish security audit reports, training certifications, and performance metrics as part of this structured annual assessment.

Lastly, the ISO is responsible for developing security policies and procedures. These policies are intended to monitor and ensure consistency across the security office, thereby improving the overall security of the organization.

Control: Compliance and Regulatory Oversight

ISO, BSB, and OLA are working to improve our information security policies to ensure proper compliance and regulatory oversight. These revised policies will better support our computer systems and ultimately our consumers.

Some examples of improvements include how we screen and select third-party contractors; ensuring we take into consideration their reputation, experience, and track record. Revising our solicitation templates, which are requirements for the third-party, will help us better educate prospective contractors before they are awarded a contract. This includes creating service-level agreements, identifying performance metrics, specifying security and compliance requirements, provisions for termination, penalties and dispute resolution, and defining data handling and protection requirements well in advance of executing a contract.

Control: Resumption Strategies

ISO, BSB, and OLA will refine our business continuity, technology recovery, and disaster recovery plans. These refinements aim to align with service-level agreements and contract terms. This also encompasses provisions for covering costs arising from contract breaches or emergency vendor deployment, should the third-party contractor be unable to promptly resume business operations.

Our contracts will incorporate elements from our technology recovery plan. This includes all Covered California third-party contractor systems, service-level agreements, recovery time objectives, and resumption strategies. By improving our contractual terms, we will be able to provide transparency to employees and third-party contractors alike on the precise steps and expectations concerning system recovery in the event of disruptions or disasters. This ensures that all parties involved understand the agreed-upon measures for restoring functionality, minimizing downtime, and swiftly resuming operations in unforeseen circumstances.

CONCLUSION

The California Health Benefit Exchange 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.

Jessica Altman, Executive 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