

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date

2025-04-16

2. Department

California High-Speed Rail Authority

3. Organizational Placement (Division/Branch/Office Name)

Financial Office

4. CEA Position Title

Enterprise Risk Director

5. Summary of proposed position description and how it relates to the program's mission or purpose. (2-3 sentences)

Under the general direction of the High-Speed Rail Authority's (Authority) Chief Financial Officer (CFO), the Enterprise Risk Director is responsible for leading the Authority's Enterprise Management Branch, which includes the Enterprise Risk Management (ERM) program, Capital Insurance program, Quality Process Management function, Internal Controls Management function, and Committee Governance. The position will advance the Authority's internal control framework, through the management of these core functions which together work to ensure stability and integrity by integrating governance, risk management, and operational effectiveness across the organization. The incumbent will provide day-to-day management for each functional area and will be responsible for the development and maintenance of policies, procedures, manuals, and instructional documents that govern their processes and strategies. In addition, the Enterprise Risk Director will serve as a trusted advisor to executive leadership and the Board on risk related matters to drive informed decision-making.

6. Reports to: (Class Title/Level)

Chief Financial Officer, Exempt

7. Relationship with Department Director (Select one)

- ☐ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.
- ☒ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(Explain):

This position supports each Executive Management team member with development of their risks, issues, and management mitigations. This position also will be the Administrator for the Enterprise Risk Committee, where the CEO is the Chair and reports are provided to the Board.

8. Organizational Level (Select one)

- ☐ 1st ☐ 2nd ☒ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

The Enterprise Risk Director (CEA B) is responsible for the development, administration, and implementation of the Enterprise Risk Management program, the Capital Insurance program, the Quality Oversight Process Management function, the Internal Governance Management, and the Internal Controls Management function.

The CEA B will be responsible for the policy and associated procedure setting for enterprise risk management. This includes the enterprise risk management plan, which is the operational tactics for functional areas and requires annual updates and submission to the Federal Railroad Administration (FRA). In addition, this position is responsible for setting policy for the Capital Insurance and Quality Oversight Process Management Section and the Committee Oversight and Coordination Section. Finally, the CEA B will be responsible for establishing new policies and procedures for Internal Controls management within the organization, which must be in compliance with the State Leadership Accountability Act (SLAA).

The CEA B will be responsible for the staffing and workforce development of the Enterprise Management Branch, including state staff from multiple bargaining units and professional consultant staff. The CEA B will be required to become an Authority Contract Manager, responsible for the Authority's Risk Advisor contract valued at over \$6 million currently.

The CEA B will be responsible for monthly coordination, preparation, and development of reports for the Board of Directors' monthly Finance and Audit Committee meetings.

The CEA B will be responsible for the collection of project risk information, as it pertains to the \$6.8 billion in federal grant funds for the monthly risk update meeting with the FRA. The CEA B will be required to collect information from all project managers, analyze and distill the information down to only grant scope of work (many Authority projects contain scope elements not applicable to the multiple grants), verify the data's accuracy against source data, create the monthly report, and brief the FRA in the monthly meetings.

The CEA B will be responsible for the day-to-day management of the Enterprise Management Branch, which consists of:

- Enterprise Risk Management Section: Develop, implement, and operationalize the enterprise risk management functions, including the overall enterprise risk management activities, systems, tools and support of program and project risk managers. In addition, this Section administers the Authority's Enterprise Risk Committee, which meets monthly and creates an annual Enterprise Risk Register. Further, collaboratively interacts with executives, functional directors, and others to support risk management objectives. Finally, meets monthly with the Audit Office to promote the three-lines-of-defense management support function (Management is the first line, Risk is the second line, and Audit is the third).
- Capital Insurance and Quality Oversight Process Management Section: As two distinct units, the Capital Insurance function is responsible for supporting all contracting and risk transfer structuring for major scopes of work and responsible for creating and administering the Authority's Owners Controlled Insurance Program. Further, this function also conducts routine compliance checks of contracted entities' insurance requirements (over 200 contracts managed). The Quality function is responsible for the quality management program, including the policy and procedures, ISO9001:2015 compliance, and Non-Conformance Report system (construction quality database). In addition, this quality function performs routine audits and reviews across the enterprise for quality compliance and ISO compliance.
- Committee Oversight and Coordination Section: Performs administration of Authority governance committees, including the Business Oversight Committee (Baseline control board and funding commitments) and the Program Delivery Committee (trends, risk, and performance of the project). While the Program Delivery Committee reviews, monitors, and creates an accountability for program trends, the BOC reviews change control committee decisions, assess the adequacy of proposed changes, authorizes new contracts, and ensures the appropriate and effective use of public funds. In addition, this group provides analytical support for various deliverables like the Organizational Management Plan and Project Management Plans.

This CEA B must develop a new Internal Controls Management Section/Unit. The Authority, as a state department, has certain requirements for internal controls and with the growth of the project and the increasing size of the department the need for a dedicated team to manage the documentation, systems, and reporting of internal controls is necessary. Internal controls are a component of the First Line of Defense in an organizations' structure of risk and control duties, which generally follow Green Book's 17 principles and 5 Components of internal control to comply with state and federal rules, regulations, and laws for combating fraud, waste, and abuse of limited public funds. In short, the 17 principles work together to create an effective control system. A lack of one of the principles can significantly affect the system as a whole. Continuous assessment of the Authority's adherence to management controls (e.g., internal control for record keeping, control for communications, control for approvals/decisions, physical and systems access) is the only way to ensure they are effective. If a principle or component is not effective, or the components are not operating together in an integrated manner, then an internal control cannot be effective and the likelihood of fraud, waste, or abuse increases.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

- ☒ Program is directly related to department's primary mission and is critical to achieving the department's goals.
- ☐ Program is indirectly related to department's primary mission.
- ☐ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: The programs associated with this request are critical to the mission and purpose of the Authority. As a result of the CEO's strategy changes, the Financial Office responsibilities have grown and more stringent demands on controlling program risk and costs are required. With significant challenges constantly arising from unknown instances in construction, and the need for more robust risk management, the Authority's risk function is increasing its capabilities to provide more timely support to achieve goals and reduce the uncertainty for risk that potentially can materialize into hundreds of millions of dollars in increased costs. Further risk management and internal controls management is required by state law for every department. The Authority is required to report on its risk management systems and how its management controls are preventing fraud, waste, and abuse. This request supports the Authority's efforts in these endeavors by having a high-level policy maker who will focus on these critical efforts to test Authority controls and advise on changing controls if variances are found. Policy and critical decisions must also be made by this key leadership position to develop new controls when gaps are identified, and report on the sufficiency controls to manage risk and issues. To provide some examples, the Authority has controls in place for purposes such as ensuring commitment of funds follows a described and documented process, ensuring invoices are tied back to a contract and an authorized representative, ensuring critical Information Technology (IT) controls for spam and cyber attacks, etc.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

The Authority is requesting the creation of the Enterprise Risk Director, within the Financial Office, to align with the duties and requirements as set forth for the Financial Office with the recent reorganization of the Authority's internal management structure. In late 2024, Governor Newsom and the Authority Board of Directors announced a new CEO for the Authority. The new CEO, once on board, set out to re-structure the Authority into a more effective program delivery organization. In January 2025, the CEO released a new vision for the organization with a re-organized structure. The new vision sets out several new mandates (managing risk across the organization, SLAA, and internal controls) for the Financial Office, which has resulted in the need for a CEA B to be created to support the CFO in leading the Enterprise Management Branch.

While the above actions seek to drive significant change in delivering the program the functions that support and manage risk and controls also increase; a vital function in an ever-challenging environment to stay on time and budget, the Enterprise Management Branch functions are state mandated (SLAA) activities and also growing.

The Enterprise Management Branch, with its three core functions: 1. Capital Insurance and Quality Management Section, 2. Committee Oversight and Coordination Section, and 3. Enterprise Risk Management Section more appropriately align with the duties and responsibilities under the CFO and the Financial Office, rather than the Project Controls Office. For instance, the Committee Oversight and Coordination Section supports the Business Oversight Committee and that committee is chaired by the CFO. Also, in the Capital Insurance and Quality Management Section, the primary role of this section is to develop an Owner Controlled Insurance Program which is a financial tool for controlling insurance costs and transferring risk. The Enterprise Risk Management section provides the radar for the organization providing the CFO early warning of financial risks and issues, as well as supports the SLAA reporting requirement housed with the CFO. Lastly, the Authority is developing a new Internal Controls Management Section (the CEA B would lead this effort), which aligns with the CFO's responsibility for the financial controls of the department. These controls include, but are not limited to, separation of duties, physical controls, standardized documentation, reconciliations, and financial policies and procedures as they relate to the associated risks: invoicing fraud, over/under payments, timely payment regulations, safeguarding assets, access to financial systems, reporting inaccuracies and risk of not detecting errors, fraud or theft.

Lastly, the Authority CFO is the primary liaison with the newly created CAHSR Office of Inspector General (OIG) and fields the majority of the questions, review reports, and response coordination for the OIG. This additional workload is growing and this CEA B will support the CFO in being responsive and timely with information for the OIG needs.

Financial Office staff is unable to absorb this entire branch and the activities it conducts, therefore the addition of the requested CEA B is necessary.

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

The CEA B is responsible for all policies, procedures, manuals, and job aides/templates contained within the Authority's Enterprise Management Function, Capital Insurance program, Quality Oversight, and Committee governance. In addition, the CEA B would be developing the Authority's first internal control management policy, procedure, and manuals to support management's responsibilities to combat fraud, waste, and abuse (in conjunction with the Internal Audit function and conformance with SLAA requirements). Examples include:

1. POLI-1103 – Enterprise Risk Management Policy: the purpose of this policy is to establish the formal acknowledgment, acceptance, and commitment of the Authority to participate in and contribute to the Enterprise Risk Management (ERM) function. Through this policy the Authority strengthens its system of internal controls and formalizes the mission and vision for the Authority's ERM function.
2. PROC-1047 – Enterprise Risk Management Procedure: this Procedure establishes the formal process for Enterprise Risk Management (ERM) and serves as a guide for management and staff as they manage risks within their respective roles and stewardship. This Procedure further outlines the governance, tools, and leading practices to enhance the efficiency, transparency, and accuracy of risk information and reporting.
3. PLAN-1015 – Enterprise Risk Management Plan: this plan provides the foundation and a set of principles that guides the development and implementation of the Enterprise Risk Management Program. This plan also sets forth a target operating model aligned with COSO's Three Lines of Defense Model, thus equipping executive leadership, management, and staff with the necessary support, and capabilities to identify, assess, manage, and report risks effectively (i.e., management and operations teams as first line of defense, risk, legal, and quality as a second line of defense, and audit as the third line of defense). Another key purpose of the Plan is to provide guidance, processes, and tools that strengthen the Authority's first line of defense for risk management so they can better manage and respond to risks within their domain. Finally, this plan sets forth the framework of how the the Risk Management Section coordinates efforts with Internal Audits (the third line of defense) to ensure that the Authority's strategic direction and risk monitoring activities are aligned with appropriate standards.
4. POLI-1006 – Quality Policy: The purpose of this policy is to establish the Authority's commitment to creating a Quality Management System (QMS) in accordance with generally accepted industry practice and to ensure the Authority implements a QMS throughout the organization.
5. MANUAL-1000 – Quality Manual: the purpose of this document is to develop a QMS to provide products and services that consistently meet program requirements and promote ongoing Continuous Improvement. The MANUAL-1000: Quality Manual defines the Quality Management Oversight Team's (QMOT) role in supporting the Authority's mission, vision, and goals; the 2022 Business Plan (BP); and Operations Management Plan (OMP). This document serves the purposes of both the MANUAL-1000: Quality Manual (QM) and MANUAL-1000: Master Quality Plan (MQP). The QMOT provides the required Leadership and support to attain a certified QMS in accordance with the International Organization for Standardization (ISO) 9001:2015 – Quality Management Systems Requirements that aligns with the Authority's business and program objectives.
6. SLAA: under the SLAA, heads of state entities are responsible for establishing and maintaining a system of internal control within their organizations. Internal control means a process to provide reasonable assurance that the objectives of an entity will be achieved. State agencies are responsible for reporting the adequacy of the entity's internal control and monitoring practices through their: control environment, risk assessment, control activities, information/communication, and monitoring.
7. Internal Control Management Policy and Procedures to be developed under this CEA B to create the framework of adherence to the Green book's 17 principles of effective internal control systems and the requirements of Authority management. In addition, the tools and templates to assist with continuous assessments and cooperative structure with Internal Audits and the OIG for management controls and incident reporting. The CEA B must establish a manual for staff to set expectations on a new process of annual assessment of internal controls and the effectiveness of those controls or needs to modify. Communication plans for documenting and assessing processes, management will need consider "what could go wrong" with the processes in place and how the controls should be designed to mitigate risk.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

The CEA's scope is enterprise-wide ranging from risk, insurance, controls, and governance policy across the organization. The incumbent serves as an experienced leader responsible for the development, management, maintenance, and revision of the Authority's Enterprise Management function, Capital Insurance Program, Committee Governance, Quality Management Oversight and develops new Internal Controls Management. The CEA B will have broad authority over the policy making in each of these areas (see list in Question 26 response).

The CEA will also be the administrator of the monthly Enterprise Risk Committee. In addition, the CEA will assess and analyze management actions to respond to risk and issues related to achieving strategic goals and objectives. The CEA will provide expertise and advice on best practices for qualitative expressions of risks and issues, including severity, impact, and velocity. Further, the CEA will support the quantitative assessments of key strategic risks and their impact on revenues and costs. Lastly, the CEA will be responsible for the Authority's development of its annual enterprise risk register, with management actions to address those risks, priority, and reporting of those risks to the Board of Directors.

Within the Capital Insurance Program, the CEA will lead specific efforts to craft risk transfer provisions, compliance requirements and threshold levels of coverage for major procurements. The CEA will lead their team in administering the Authority's Owner Controlled Insurance program, where two lines of coverage will reside. The first line of coverage will be Commercial General Liability coverage to satisfy the class 1 railroad requirements. The Authority will have one umbrella policy to cover all future construction contractors. The second line of coverage will be railroad protective liability coverage with limits up to \$25 million. The CEA will also oversee and conduct studies on potential additions of other lines coverage, such as Contractor Pollution Liability.

The CEA will be responsible for the administration of the monthly Business Oversight Committee, supporting the CFO by reviewing, evaluating, analyzing, and recommending funding requests for decision making.

The CEA will oversee the Quality Process Management Section to ensure Authority quality processes are being adhered to and non-conformances are tracked, reported on, and followed up on through resolution.

Lastly, the CEA will responsible to build the Authority's Internal Control Management section.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

Yes, the CEA B is responsible for all polices, procedures, manuals, and job aides/templates contained within the Authority's Enterprise Management Function, Capital Insurance program, Quality Oversight, and Committee governance. In addition, to the above the CEA B would be developing the Authority's first internal control management policy, procedure, and manuals to support management's responsibilities to combat fraud, waste, and abuse (in conjunction with the Internal Audit function and conformance with State Leadership Accountability Act requirements).