CalHFA California Housing Finance Agency

Public Meeting Agenda

California Housing Finance Agency
Audit and Risk Management Committee
Thursday, November 19, 2026
9:00 a.m.

Public Meeting Location:
500 Capitol Mall
14th Floor Main Conference Room
Sacramento, CA 95814

This meeting is open to the public pursuant to Government Code Sections 11120-11132.

The meeting is available in-person and via Zoom. Public comments may be made in-person or through Zoom.

Click here to register on Zoom:
CalHFA Audit and Risk Management Committee Meeting – November 19, 2026

1. Roll Call
2. Approval of the minutes of the February 19, 2026 meeting 1
3. Chairperson's comments
4. Enterprise Risk Management framework update (Kelly Madsen) 3
5. Annual Review of the Committee Charter 28
6. Other committee matters
7. Public comment: Opportunity for members of the public to address the Committee on matters within the Committee's authority
8. Adjournment

NOTES:

Parking: Public parking is available at the 500 Capitol Mall parking structure, with the entrance located on N Street.

Parking is managed via the Metropolis Parking App:

1. Go to **metropolis.io** or download the Metropolis Parking app.
2. Create an account.
3. Add your license plate number and payment method.

Cameras will automatically read your license plate upon entry and exit — no tickets or kiosks needed. Your payment will be processed automatically.

Refreshments: Available nearby, at Panera and Old Soul Coffee

MINUTES

California Housing Finance Agency (CalHFA)
Audit and Risk Management Committee Meeting
February 19, 2026
Meeting noticed on Friday 6, 2026

1. Roll Call

The California Housing Finance Agency Audit Committee meeting was called to order at 9:00 a.m. by Chair Williams. A quorum of members was present.

MEMBERS PRESENT:	Wiant (for Ma), White, Williams
MEMBERS ARRIVING AFTER ROLL CALL:	None
MEMBERS ABSENT:	None
STAFF PRESENT:	Tony Sertich, Claire Tauriainen, Erwin Tam, Oksana Glushchenko, Courtney Pond
GUEST SPEAKERS:	Mandy Merchant, Principal, CliftonLarsonAllen, LLP.
	Elizabeth Richarson, Senior Audit Associate, CliftonLarsonAllen, LLP.

2. Approval of the minutes – January 22, 2026

On a motion by White, the minutes were approved. The vote was as follows:

AYES:	Wiant (for Ma), White, Williams
NOES:	None
ABSTENTIONS:	None
ABSENT:	None

3. Chairperson comments

Chair Williams thanked Board Chair Cervantes for the opportunity to serve as the newly appointed Committee Chair and expressed his commitment to accountability and transparency.

4. Review and discuss the Audited Financial Statements for the California Housing Finance Fund for the year ended June 30, 2025, including a discussion with the principal from CliftonLarsonAllen, LLP.

Presented by Merchant and Richardson

Merchant and Richardson provided the Committee with an overview of the audit results of the California Housing Finance Fund. They reported that the Agency received an unmodified or "clean" opinion for both the GAAP financial statements audit and the Single Audit. They reported that the agreed-upon procedures from the compliance audit of the MyHome and California Dream for All programs revealed no findings.

5. Other Committee matters

Chair Williams asked if there were any other matters to discuss and there were none.

6. Public comment

Chair Williams asked if there were any members of the public who wanted to provide a comment and there were none.

7. Adjournment

As there was no further business to be conducted, Chair Williams adjourned the meeting at 9:37 a.m.

MEMORANDUM

To: Board of Directors **Date:** November 19, 2026

From: Kelly Madsen, Director of Enterprise Risk Management & Special Initiatives
California Housing Finance Agency

Subject: Agenda Item 4– Enterprise Risk Management Framework Update

Purpose

The purpose of this item is to present the Audit and Risk Management Committee with the first look of the newly documented Enterprise Risk Management (ERM) framework. While most of CalHFA's risk management and compliance processes have been in place for some time, those processes have not been clearly recorded into one document until now. This item supports the Audit and Risk Management Committee in meeting their responsibility in reviewing and recommending changes to the board to the ERM Framework.

Recommendation

Staff recommend that the Audit and Risk Management Committee receive and review the Enterprise Risk Management framework and provide any questions on the framework and its ongoing implementation.

Executive Summary

The Board delegated oversight of the ERM framework to the Audit and Risk Management Committee through its charter. As part of CalHFA's commitment to effective governance, organizational resilience, and sound stewardship, the ERM framework establishes a structured and consistent approach to identifying, assessing, responding to, and monitoring risks that could affect the Agency's strategic objectives and mission.

The ERM framework aligns CalHFA's risk management practices with the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] Enterprise Risk Management framework, an industry-recognized standard for effective risk management and organizational resilience. By documenting enterprise risk management principles, governance, roles and responsibilities, and reporting expectations in a single governance document, the ERM framework strengthens oversight, accountability, and risk-informed decision-making across the Agency.

By documenting the ERM framework, we can:

- **Strengthen organizational resilience and preparedness** by establishing a consistent process for identifying, assessing, responding to, and monitoring enterprise risks.
- **Enhance risk-informed decision-making** by providing leadership with clear and timely information concerning significant risks and risk response activities.
- **Align risk management with strategy and objectives** by considering risk as part of strategic planning, operational decision-making, and mission delivery.
- **Clarify governance and strengthen accountability** by defining risk management roles and responsibilities across the Audit and Risk Management Committee, executive leadership, the Enterprise Risk Management & Special Initiatives Division, and Agency business areas.
- **Promote transparency and communication** by establishing expectations for communicating and reporting relevant risk information.
- **Support continuous improvement** by providing a structure for periodically reviewing and enhancing the Agency's risk management practices.

The ERM framework is intended to serve as a living governance document. As CalHFA's operating environment, strategic priorities, and risk landscape evolve, the ERM framework will be periodically reviewed, refined, and enhanced to support the Agency's long-term resilience and effectiveness.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an organization dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the American Accounting Society, American Institute of CPAs, Financial Executives International, Institute of Management Accountants, and the Institute of Internal Auditors. Applying the COSO ERM Framework

Key Changes

As part of developing the ERM framework and advancing the maturity of CalHFA's enterprise risk management program, staff has implemented and is continuing to implement several enhancements, including:

- **Formal documentation of CalHFA's Enterprise Risk Management Framework** into a single governance document that establishes enterprise risk management principles, governance, roles and responsibilities, and reporting expectations across the Agency.

- **Enhanced enterprise risk assessment and scoring methodology** to strengthen the identification, prioritization, and reporting of enterprise risks and support risk-informed decision-making.

- **Establishment of a Risk Champion Network** to strengthen risk awareness, facilitate collaboration, and support risk management activities across the Agency.

- **Alignment of enterprise risk management activities with the updated State Leadership Accountability Act (SLAA)** annual reporting requirements to support statewide accountability and reporting expectations.

Our goal is not only to continually improve risk and compliance reporting to the Board and the Audit and Risk Management Committee as the ERM program continues to mature, but also to help ensure that CalHFA remains a resilient, accountable, and mission-driven organization in service to Californians. The ERM framework establishes the foundation for the Agency's enterprise risk management program, with its long-term success dependent upon active governance, cross-functional collaboration, regular risk assessment, transparent reporting, and continuous improvement.

California Housing Finance Agency

Enterprise Risk Management Framework

November 2026

Contents

Introduction 2

Layer 1: The Practice of Enterprise Risk Management 3

Performance: Application of the Risk Assessment 3

Risk Assessment 3

Risk Identification: How risks are identified 3

Evaluation and Prioritization: How Risks are Scored and Ranked 4

Risk Response: How to respond and react to risks 8

Risk Universe: A Bird's Eye View 9

Information, Communication and Reporting 10

How Information Flows 10

Communication of Risk 10

Reporting 11

How CalHFA Continuously Improves 13

Review and Revision 14

Layer 2: The Foundation of Enterprise Risk Management 15

Governance, Culture, & Ethics 15

Authorities and Responsibilities 15

Policies and Standards Management 18

Risk and Compliance Culture 18

Strategy and Objective-setting 19

Strategy Alignment 19

Risk Appetite 20

Risk Metrics 20

Risk Categories 20

Introduction

The California Housing Finance Agency (CalHFA) is committed to delivering reliable financing solutions that advance housing opportunities for Californians. This mission requires strong governance, financial stewardship, and operational excellence. As the housing landscape and broader operating environment continue to evolve, CalHFA must remain resilient and adaptive to ensure the agency can fulfill its mission and stay aligned with long-term strategic direction. To support this resilience, CalHFA uses a proactive, enterprise-wide approach internally known as the Enterprise Risk Management (ERM) Framework.

The ERM Framework is CalHFA's proactive, agency-wide approach for identifying, assessing, responding to, and monitoring risks that may affect the agency's mission, operations, or strategic objectives. It provides a consistent structure, promotes transparency, and reinforces CalHFA's commitment to effective risk management by clearly outlining expectations across the organization.

CalHFA's ERM Framework is built on the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[1] Integrated ERM Framework, a widely recognized model for strong risk governance and management practices. The framework incorporates five COSO components:

- Governance & Culture
- Strategy & Objective-Setting
- Performance (Risk Assessment)
- Review & Revision
- Information, Communication & Reporting

These components work together as a unified system to promote transparency, strengthen alignment between risk management and strategic planning, and help CalHFA proactively anticipate, prioritize, and respond to risks that may influence the agency's ability to effectively serve Californians.

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an organization dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the American Accounting Society, American Institute of CPAs, Financial Executives International, Institute of Management Accountants, and the Institute of Internal Auditors. Applying the COSO ERM Framework

Layer 1: The Practice of Enterprise Risk Management

With these COSO components as the structural foundation, CalHFA's ERM Framework moves into practical application. The first layer of this framework focuses on how risk management is practiced across the agency and provides guidance on the activities staff encounter during the risk assessment process.

Performance: Application of the Risk Assessment

Risk Assessment

One of the key components of the ERM Framework is the ability to perform a risk assessment to identify and respond to enterprise level challenges and risks. The ERM team maintains and administers an enterprise-wide risk assessment each year to reassess known risks and identify emerging ones. This annual assessment ensures proactive risk identification, supports regulatory requirements, and promotes strategic alignment and informed decision-making.

The risk assessment process is structured and repeatable, consisting of three integrated stages:

1. Risk Identification – Detecting risks from internal and external sources
2. Evaluation and Prioritization of Risks – Assessing the likelihood and potential impact of each risk
3. Risk Response – Comparing analyzed risks against organizational appearance to determine the appropriate treatment or mitigation.

Risk Identification: How risks are identified

Risk identification is the first essential stage in the risk assessment. It helps staff surface issues early, recognize patterns, and understand where CalHFA may face uncertainty. Risks are identified by gathering information from people, processes, and the environment in which CalHFA operates.

CalHFA uses multiple approaches to ensure risks are captured from both day-to-day operations and broader environmental trends. The following methods help staff and leadership identify risks clearly and consistently:

Methods Used to Identify and Gather Risks:

- **Environmental Scanning** – Monitoring external developments such as new regulations, economic shifts, or industry trends.

- **Interviews** – Uncover risks through one-on-one discussions, brainstorming sessions, and engagements with division experts, risk champions, and leadership.
- **Surveys and Questionnaires** – Capturing structured input through risk identification surveys to surface patterns, issues, or concerns across the agency.
- **Operational Discussions** – Identify risks revealed through team conversations, cross-divisional coordination, or recurring operational challenges.
- **Program and Project Reviews** – Identify risks through lessons-learned sessions, project evaluations, audit findings, and post-mortems

CalHFA classifies risks into three primary types to better understand their nature, urgency, and required level of response:

Existing Risks: Known risks CalHFA has encountered before or previously documented. They are supported by historical data, established processes, and institutional experience, making them generally more stable and predictable.

Emerging Risks: New or evolving risks are characterized by limited information and higher uncertainty. These risks often arise from shifts in technology, regulation, economic conditions, legislation, or industry trends and may develop quickly as CalHFA's operating environment changes.

Existential Risks: Low-probability but high-impact risks, that if realized, could require CalHFA to significantly and immediately change how it operates or delivers critical programs. These risks represent threats to CalHFA's Fundamental ability to meet its mission and may necessitate one or more major responses:

- Strategic Shifts: Redirecting or restructuring programs, processes or organizational priorities to address heightened exposure or new external realities.
- Business Continuity Management: Leveraging CalHFA's Business Continuity Management Program to sustain essential operations, protect critical functions, and maintain delivery of services under extreme or disruptive conditions.

Existential risks are often considered a subset of emerging risks, but they require elevated attention because their consequence could reshape how CalHFA functions.

Evaluation and Prioritization: How Risks are Scored and Ranked

Once risks are identified, they are evaluated using three measures: Likelihood, Impact, and Velocity. Combined, these measures determine the severity of a risk and help leadership allocate resources effectively.

Likelihood refers to the probability or expected frequency with which a risk may occur. It may be informed by historical trends, external conditions, industry reference points, or the professional judgment of risk champions. Depending on the nature of the risk, likelihood may be measured using qualitative or quantitative methods.

Likelihood		
Rating	**Probability**	**Descriptor**
1 - Rare	0% to 10%	The risk is unlikely to occur; no known occurrences would require multiple failures or unusual conditions.
2 - Unlikely	>10% to 30%	The risk could occur but not expected under normal circumstances. There are occasional historical examples but infrequent. Requires specific conditions or a triggering event
3 - Likely	>30% to 60%	The risk occurs with some regularity. There is clear evidence of past occurrences. Could happen in the normal course of business
4 - Almost Certain	>60% to 100%	Event is expected to occur frequently. There are strong indicators, repeated past occurrences, or persistent conditions. Happens regularly unless mitigated.

Figure 1. Likelihood Scale

Impact represents the consequences a risk event may have across multiple critical areas of CalHFA. When assessing impact, each risk is evaluated not only on its financial effects, but also compliance, reputational, operational, and strategic effects. Each risk is evaluated using an impact profile, a structured set of categories that capture the full breadth of potential consequences. For example, a risk may simultaneously affect CalHFA's financial stability, regulatory compliance, public reputation, and strategic objectives.

During the assessment, each dimension is rated individually (e.g., financial, compliance, reputational, strategic), and these ratings are combined to produce an overall impact score. This approach ensures that the impact assessment is comprehensive and reflects the true scope of the risk, rather than focusing solely on monetary loss. By diving deep into the impact profiles, CalHFA can prioritize risks more effectively and tailor mitigation strategies to address all areas of potential exposure.

Impact		
Score	**Impact Profile**	**Descriptor**
1	**Low**	Minor to no impact. Consequences can either be ignored or easily managed with routine procedures or minimal additional effort.
2	**Moderate**	Impact is noticeable. Consequences must be managed with additional controls or mitigation strategies. Requires attention and more resources.
3	**High**	Significant or potentially severe impact. Immediate action required. Consequences can interrupt business, performance issues, and/or cost overrun.
4	**Severe**	Severe impact. Immediate and intensive attention and efforts needed. Consequences lead to long-term damage and failures across organization.

Figure 2. Impact Scale

Impact Profile						
Score	**Financial Impact (Operating Budget)**	**Financial Impact (Agency Wide Balance Sheet)**	**Compliance (Regulatory & Legal)**	**Operational**	**Reputational**	**Strategic**
1 – Minimal	Loss or inefficiency < $10,000; minor budget variance	Loss or inefficiency < $1M minor financial impact	Minor non-compliance; no penalty or reporting requirement	Little to no disruption to operations. Unnoticeable to employees	Little to no attention or issue remains internal; no media or stakeholder attention	Slight deviation from planned targets
2 - Moderate	$10,000 - $100,000 loss/inefficiency; affects one program or project	$1M - $10M loss/inefficiency; affects one program or project	Compliance issue requiring corrective action; possible audit action	Moderate disruption; workaround possible	May attract some attention but has little to no negative impact on public perception	Moderate deviation from strategic plan; impact on key initiative or goal

3 - High	$100,000 - $1M loss or inefficiency; cross-program impact	$10M - $50M loss or inefficiency; cross-program impact	Reportable breach; regulatory scrutiny or findings; qualified audit opinion	Major disruption; partial system or process failure	Noticeable attention. Negative media attention. Public concern	Threat to core objectives; long-term strategic initiative jeopardized
4 - Severe	Greater than $1M; material threat to budget integrity	Greater than $50M; material threat to financials	Serious regulatory violation; legal action, or loss of program authority	Complete process/system shutdown; critical operations fail	Significant attention. Major media coverage; brand damage; eroded stakeholder trust	Fundamental misalignment with agency mission

Figure 2.1. Impact Profiles

Velocity refers to the speed at which a risk may materialize. Some risks unfold slowly, providing time for mitigation or contingency planning, while others occur rapidly and require immediate response. Understanding velocity helps CalHFA anticipate the urgency associated with each risk and determine how quickly mitigation actions may be needed to reduce exposure.

Velocity		
Score	**Time to Impact (days)**	**Descriptor**
1 - Slow	> 121	Slow onset. May take months to up to a year to materialize. Adequate time to react and respond.
2 - Moderate	31 - 120 Days	Medium speed. Materializes within a year but not instantaneous. There is time to partially mitigate impacts when it occurs.
3 - Fast	8 - 30 Days	May occur in a matter of days to a few weeks. Little time to react.
4 - Instantaneous	0 - 7 Days	High speed. Instant impact. Little to no time to react. (e.g. earthquake)

Figure 3. Velocity Scale

Once a risk is evaluated and scored on all three measures, the scores for each measure are combined to form CalHFA's overall risk score or risk severity.

$$(Likelihood + Velocity) \times Impact = Risk\ Severity$$

This score reflects the potential severity of each risk and is used to determine which risks warrant the greatest attention. Risks with higher scores are prioritized first, ensuring that leadership can focus resources, mitigation efforts, and oversight on the issues that pose the most significant potential impact. This structured approach to prioritization supports consistent risk informed decision making and helps align CalHFA's mitigation strategies with its strategic objectives.

Risk Response: How to respond and react to risks

After risks are evaluated and prioritized, risk response strategies are then considered to determine how each risk will be managed. The risk response step is essential to the performance cycle as it transforms the identified threats into actionable plans that protect CalHFA's objectives, resources, and reputation. CalHFA responds to risks through four methods,

- **Avoidance**: Used when there is zero tolerance for a risk to occur. Plans, processes, or activities are changed to ensure the risk does not materialize.
- **Acceptance**: Used when there is tolerance for a risk to occur and the agency is willing to continue operations with full awareness of the risk's presence.
- **Transference (Share)**: Used to shift all or part of the risk to a third party. This approach is commonly associated with insurance or contractual agreements.
- **Mitigation (Reduce)**: Used to lower the likelihood or impact of a risk through controls, safeguards, or operational adjustments.

To ensure decisions are well-supported and not made in isolation, the selection of a risk response strategy is determined through a collaborative process between ERM, risk champions, and leadership.

How a Risk Response Strategy is Selected

1. Risk Champions Review and Recommend
   ERM collaborates with Risk Champions by analyzing the risk data and information to recommend an initial response strategy grounded in operational realities and the agency's capabilities.

2. ERM Consolidates and Formalizes the Recommendation
   ERM reviews these recommendations, ensures consistency across divisions, and prepares a response summary that outlines the rationale, resource implications, and expected residual risk.
3. Leadership Validation (Cabinet)
   The Cabinet reviews the recommended responses to confirm alignment with the agency's mission, strategic objectives, and established risk appetite. This step ensures the response is neither over- nor under scaled relative to the agency's tolerance.
4. Risk Champions and Risk Owners Execute the Approved Response
   Once approved by leadership, the designated risk owner (if not a risk champion) carries out the agreed-upon response strategy. ERM sets an appropriate monitoring cadence and works with the risk owner to track progress, evaluate residual risk, and update the Risk Register accordingly.

This coordinated process ensures risk responses are transparent, appropriately scaled, informed by subject-matter expertise, and aligned with CalHFA's governance expectations.

Risk Universe: A Bird's Eye View

CalHFA maintains a Risk Universe, which serves as the agency's central repository for all identified risks. As risks move through the performance cycle of identification, evaluation, prioritization, and response, it is essential that each one is documented in a single, structured location. Recording risks in one place ensures CalHFA always has a complete and transparent view of its risk landscape.

The Risk Universe provides leadership and divisions with a bird's-eye view of CalHFA's enterprise risks, including:

- Risks that have occurred in the past
- Risks that exist today
- Emerging risks that may develop over time
- Risks that were identified but ultimately determined not to pose a threat

Maintaining a comprehensive risk portfolio helps CalHFA:

- Avoid overlooking risks, regardless of size or likelihood
- Strengthen strategic alignment by showing how risks relate to operations and objectives
- Support regulatory requirements and risk reporting cycles

- Enable consistent monitoring, scoring, and analysis across divisions

By preserving every identified risk, whether existing, emerging, or existential, the Risk Universe supports a holistic understanding of CalHFA's operating environment and reinforces the integrity of the ERM process.

Information, Communication and Reporting

After risks are assessed, responded to, and documented within the Risk Universe, CalHFA relies on strong information flows and communication practices to ensure risk insights reach the appropriate operational and leadership levels.

How Information Flows

CalHFA draws from a wide range of internal and external sources to understand its risk environment. These sources help provide context, support early detection, and inform risk assessments.

How Risk Information is Gathered

- **Operational Insights**
  Information emerges from staff discussions, meetings, and daily interactions. Divisions share observations about delays, system behavior, emerging concerns, or changes in workload.
- **Division Expertise**
  Risk Champions, SMEs, and operational staff offer detailed insight into division specific risks based on their experience and responsibilities.
- **ERM Engagement**
  ERM gathers information through interviews, discussions, surveys, and identification activities conducted across the agency.
- **External Sources**
  Regulatory updates, statewide guidance, industry publications, and information from other public sector organizations support environmental awareness and help identify emerging risks.

These information channels allow CalHFA to maintain a well-rounded and timely understanding of its risk environment.

Communication of Risk

CalHFA uses open communication practices to ensure risk information is shared clearly and reaches the appropriate levels.

How Risk Communication Occurs Across CalHFA

- **Team and Cross Divisional Discussions**
  Divisions routinely talk through operational challenges and risks, allowing information to move across groups naturally and consistently.
- **Leadership Dialogues**
  Risk insights flow upward through conversations between divisions, Risk Champions, and leadership. These channels help ensure leadership visibility into areas needing attention.
- **Lessons Learned and Staff Meetings**
  Structured meetings provide opportunities for staff to share challenges, raise concerns, and discuss impacts openly and collaboratively.
- **Open-door Policy**
  CalHFA's open-door policy creates pathways for staff to elevate observations directly to supervisors or leadership whenever needed.

These practices help risk information move freely throughout the organization.

Reporting

Internal Reporting

Reporting enterprise level risks is a vital part of the ERM Framework. Regular reports are provided to the Cabinet, the Audit and Risk Management Committee, and the Board to ensure leadership has clear visibility into CalHFA's risk profile, emerging issues, and mitigation progress. Through structured reporting practices, the ERM team consolidates risk information gathered from assessments, programs, and internal controls to support timely and informed decision-making. Consistent reporting cycles ensure that leadership receives updates on key risks, trends, and changes in exposure, while divisions remain aware of expectations that promote accountability and alignment. These reports help maintain coherence between CalHFA's risk management activities and organizational objectives and ensure that significant issues are escalated appropriately across operational and strategic levels.

Reporting Cadence		
Meeting	**Schedule**	**Topics**
Audit and Risk Management Committee	Biannually; additional meetings possible if needed	• ERM Framework and ERM program charters. • Annual risk assessment reports. • Education on risk related topics. • ERM program workplans and progress updates. • Annual enterprise risk training results. • External auditors report on the adequacy of financial statements. • State Leadership Accountability Act (Reported every odd year)
Cabinet – Quarterly Business Review	Quarterly	• Enterprise risk assessment results and findings. • Emerging and existing risks affecting strategic plan and business plans. • Annual enterprise risk training results. • ERM program updates. • Recommendations to continuously improve the ERM program.
Risk Champions Network	Monthly	• Discuss and consider emerging and existing risks threatening strategic objectives. • Review and update enterprise level risks and risk metrics • Discuss and implement ERM initiatives

Figure 4. Reporting Cadence

External Reporting

The State Leadership Accountability Act[2] (SLAA) requires state entities to maintain effective internal control systems, monitor these controls on an ongoing basis, and report on their adequacy. SLAA is fulfilled through the submission of a biennial report to the Department of Finance. The ERM team incorporates SLAA requirements into the enterprise risk assessment process and works closely with executive leadership, upper management, and divisions to collect the necessary risk and internal control information. This coordinated effort ensures that CalHFA's SLAA reports accurately reflect the agency's risk environment and demonstrate compliance with statewide governance and accountability standards.

How CalHFA Continuously Improves

Continuous improvement strengthens CalHFA's ability to manage risks effectively and refine its risk assessment processes over time. The agency uses several practices to learn from experience, adapt methods, and continuously enhance the quality and consistency of risk management. Staff and divisions often draw on these practices to refine their own work and contribute to a resilient organization.

- **Reflective Learning**
  Divisions review prior projects, operational challenges, and assessments to identify insights, recurring themes, and opportunities for adjustment. Lesson-learned conversations contribute to improved planning and reduced risk exposure.
- **Structured Check-Ins**
  Teams incorporate regular check-ins to monitor progress, surface concerns, and adjust plans when conditions change. These discussions promote transparency and help refine ongoing work.
- **Cross-Divisional Collaboration**
  Divisions coordinate with one another when facing familiar or interconnected challenges. Sharing operational experiences supports early risk detection and helps clarify how issues may affect other areas.
- **Process Tools and Documentation**
  Checklists, desk guides, and written procedures are used to promote consistency. When gaps or inefficiencies become visible, divisions update materials to strengthen continuity and reduce future risk.

[2] The State Leadership Accountability Act (SLAA) requires state agencies to establish and maintain systems of internal control and to annually evaluate and certify the adequacy of those controls. Cal. Gov. Code §§ 13400-13407.

- **Post-Event Reviews and Discussions**
  After major events or initiatives, teams conduct post-mortem reviews to understand impacts, contributing factors, and opportunities to improve. These reviews help refine approaches to future work.
- **Ongoing ERM Program Evaluation**
  ERM performs annual reviews of its programs, including the enterprise risk assessment, reporting practices, tools, and templates. These reviews help ensure CalHFA's risk management approach continues to mature and respond to agency needs.

These practices form the basis of CalHFA's continuous improvement culture. Staff and divisions often apply these habits in their own work, strengthening operational quality and contributing to a proactive risk environment.

Review and Revision

While continuous improvement strengthens the quality of day-to-day risk practices, Review and Revision ensures that insights gathered across the risk assessment cycle inform the ongoing refinement of the ERM Framework itself. This governance level review keeps the framework aligned with CalHFA's evolving needs and strategic priorities.

Review and revision keep CalHFA's ERM Framework effective and responsive. Insights from the performance cycle, continuous improvement practices, and reporting activities inform periodic evaluations of the framework. These evaluations help CalHFA adjust methods, refine tools, and ensure alignment with strategic objectives and the agency's evolving operating environment. Through this ongoing feedback process, the ERM Framework remains resilient, adaptive, and reflective of CalHFA's commitment to proactive risk management.

Layer 2: The Foundation of Enterprise Risk Management

After understanding how CalHFA practices enterprise risk management through the activities in layer 1, the second layer of the ERM Framework introduces the foundational components that make those practices possible. These elements define the governance, roles, culture, and strategic alignment that support, reinforce, and sustain ERM across the agency.

Governance, Culture, & Ethics

Governance establishes CalHFA's tone and reinforces leadership's responsibility for overseeing enterprise risk management, ensuring that risk information is communicated, understood, and acted upon across the agency. Culture reflects the values and behaviors that shape how employees approach risk, emphasizing transparency, accountability, and ethical decision-making. Ethics guide staff conduct and support a professional environment where risks are addressed proactively, and concerns can be raised without hesitation. Together, these elements create a strong foundation for CalHFA's ERM Framework and ensure that risk management practices are consistently applied throughout the organization.

Authorities and Responsibilities

Effective enterprise risk management begins with strong leadership. At CalHFA, the Audit and Risk Management Committee and the Cabinet establish the tone and culture for risk management by setting expectations for governance, oversight, accountability, and transparency. Their leadership reinforces the importance of risk awareness across the agency and ensures that all groups supporting the ERM Framework understand their roles in identifying, managing, and communicating risks. The following groups collectively contribute to CalHFA's risk governance structure and support the consistent application of risk management practices throughout the organization.

Members	Role	Risk Responsibilities
Audit and Risk Management Committee	Governance	• Oversight & Advisory
Cabinet	Governance	• Oversight • Review • Strategy and Implementation
Enterprise Risk Management and Special Initiatives	Control & Assurance Function	• Framework Administration • Risk Management & Compliance
Risk Champions	Risk Owners	• Identification, Assessment, & Mitigation of Risks • Risk Reporting

Figure 5: Summary of key groups that support the ERM Framework

The **Audit & Risk Management Committee** holds the responsibility of overseeing CalHFA's financial reporting, accounting, and enterprise risk management. The Audit and Risk Management Committee serve in an advisory capacity concerning the ERM Framework.

The **Cabinet** refers to CalHFA's executive leadership. CalHFA's Cabinet holds the responsibility of governance and oversight of the ERM Framework. The Cabinet aids in defining, establishing, and monitoring risk governance and risk culture within CalHFA. Oversight and review of the ERM Framework are carried out through meetings, discussions, and communication facilitated by the Director of ERMSI.

The **Enterprise Risk Management** team leads the overall design, administration, and execution of the ERM Framework. ERM serves as the Framework's control and assurance function. ERM is responsible for the ongoing enterprise risk management process and ensures that all relevant information is communicated between the Cabinet and the business areas.

Risk Champions refer to internal staff from each division and business area who are experts in their divisions' day-to-day operations, tasks, responsibilities, and strategic goals. Their role in the ERM Framework derives from their expertise in their respective business areas, meaning that risk champions understand the various risks associated with their divisions' operations. Risk champions work with the ERM team through meetings, discussions, and ongoing communication to identify risks and ensure that the ERM Framework reflects all areas of CalHFA.

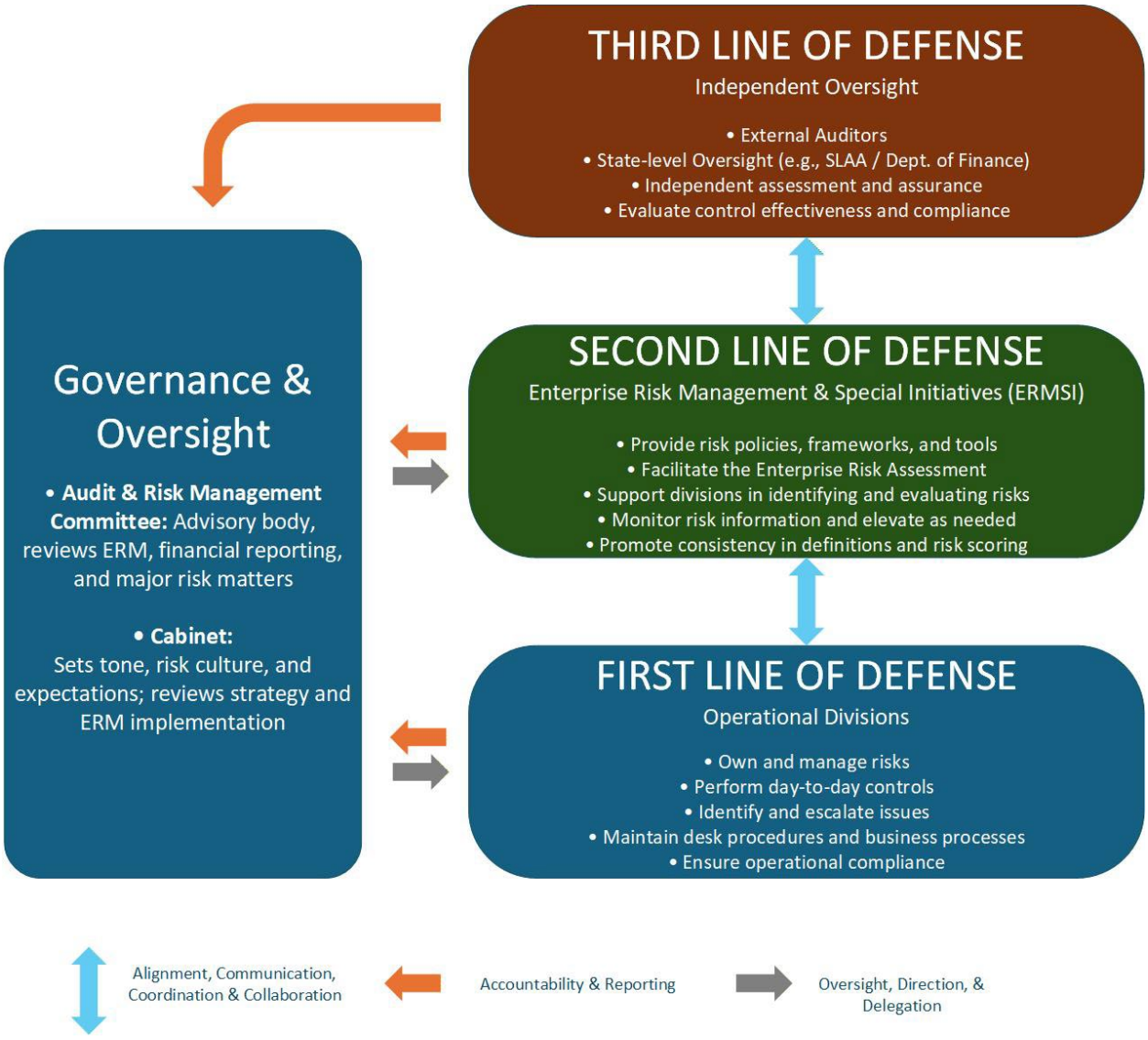

Figure 6. CalHFA Governance Structure

CalHFA's governance structure aligns with the Three Lines of Defense model, which clarifies how risk is owned, supported, and independently reviewed across the agency. The

first line of defense consists of CalHFA's divisions and business areas, which identify and manage risks as part of their daily operations. The second line of defense is the Enterprise Risk Management and Special Initiatives (ERMSI) team, which provides the Framework's, tools, guidance, and monitoring needed to support divisions in managing risk. The role of **the third line of defense** is fulfilled through independent oversight mechanisms such as external auditors and state level review bodies (e.g. Dept. of Finance, Dept. of Technology, State Auditor), which collectively provide objective evaluation of CalHFA's risk and control environment.

Policies and Standards Management

Policies help CalHFA document and communicate the behaviors, requirements, and expectations, that guide consistent and responsible operations across the agency. Effective policy and standards management ensures that CalHFA's policies remain current, relevant, and aligned with industry best practices, applicable federal and state laws and regulations, and the agency's core values. ERMSI collaborates with all business areas within CalHFA to manage policies and standards. This collaboration ensures that all CalHFA staff have access to and understand the rules, expectations, and best practices within CalHFA, which promotes risk and compliance culture.

Risk and Compliance Culture

CalHFA's risk and compliance culture is grounded in the agency's long-standing values of accountability, ownership, transparency, and integrity. These values guide how employees approach challenges, make decisions, and support one another through complex issues. The organization has historically demonstrated a proactive mindset toward risk: staff openly discuss challenges during meetings, share emerging concerns early, and communicate operational impacts across divisions through established channels. These behaviors reflect a culture where risk awareness is part of everyday work, even outside of formal ERM processes.

CalHFA also maintains an environment that encourages open dialogue and cross-functional collaboration. An open-door approach to communication allows staff to surface questions or concerns directly to leadership, ensuring that risks are recognized before they escalate. Divisions regularly coordinate when faced with familiar or recurring challenges, relying on designated groups and experienced teams to troubleshoot issues quickly and effectively. These habits support operational continuity and demonstrate the agency's existing strength in navigating uncertainty.

To reinforce the agency's risk and compliance culture, the ERM team collaborates with divisions to deliver enterprise risk management training that promotes awareness of staff

responsibilities related to risk. This training strengthens thoughtful decision-making and enhances organizational resilience. The ERM team further supports staff through educational sessions held during enterprise risk management activities, providing clear explanations of the purpose, goals, and expectations of each process. These briefings help ensure that staff share a common understanding of the work at hand and build knowledge beyond basic risk management concepts, including areas such as business continuity planning and risk analysis.

As the ERM Framework matures, it reinforces these cultural strengths by providing consistent tools, shared language, and structured practices that complement CalHFA's already proactive approach. This alignment helps embed a risk-aware perspective into daily operations and ensures that staff at all levels have the confidence and clarity needed to identify, communicate, and address risks in support of CalHFA's mission.

Strategy and Objective-setting

Enterprise risk management, strategy, and objective setting work together to support CalHFA's long-term goals and operational priorities. This component of the ERM Framework ensures that risk considerations are incorporated into the agency's planning activities, enabling leadership to make decisions that align with CalHFA's mission and risk tolerance. Integrating ERM with strategic planning allows CalHFA to better anticipate challenges, optimize opportunities, and maintain a clear line of sight between risk, performance, and strategic objectives.

Strategy Alignment

Strategy alignment ensures that CalHFA's risk management practices support the development and execution of the agency's strategic and business plans. Risk considerations help inform strategic decisions by clarifying potential challenges, dependencies, and impacts that may influence agency priorities. The ERM team collaborates with divisions and leadership to evaluate risks that may affect strategic initiatives, ensuring that planning efforts remain grounded in realistic assumptions and account for emerging conditions. This alignment strengthens the agency's ability to achieve its goals while maintaining stability and operational effectiveness. To further support strategic planning, the ERM Framework and enterprise risk assessment provide key insights that inform decision-making during CalHFA's Quarterly Business Reviews, ensuring leadership has timely and relevant risk information when evaluating progress and setting priorities.

Risk Appetite

Risk appetite defines the level and types of risk CalHFA is willing to accept in pursuit of its mission and strategic objectives. Establishing risk appetite provides a shared understanding of acceptable exposure levels and serves as guidance for decision-making, resource allocation, and prioritization. Risk appetite helps ensure that risk-taking activities remain within appropriate boundaries, supporting both compliance requirements and CalHFA's commitment to ethical and responsible operations. The risk appetite may be adjusted over time to reflect changes in the business environment, regulatory landscape, or agency priorities.

The Cabinet is responsible for establishing CalHFA's risk appetite by evaluating the agency's strategic goals, operational needs, and overall risk tolerance. Through ongoing review and consultation with the ERM team and risk champions, the Cabinet defines and refines the organization's appetite for various types of risks to ensure alignment between CalHFA's mission, resources, and long-term objectives. Following the Cabinet's establishment of the risk appetite, the Audit and Risk Management Committee reviews and approves the proposed risk appetite as part of its oversight role, ensuring alignment with CalHFA's governance expectations and the broader ERM Framework. This governance role ensures that risk appetite remains current, actionable, and embedded in the agency's decision-making processes.

Risk Metrics

Key Risk Indicators (KRIs) are metrics used to help CalHFA monitor key risks, identify trends, and detect changes in exposure. These metrics may be quantitative or qualitative and are selected for their alignment with CalHFA's strategic goals and operational needs. They promote accountability by ensuring risks are tracked consistently and transparently across divisions. Risk Champions collect KRI data and submit it to the ERM Team each quarter for review, assessment and reporting to leadership. KRIs also help leadership determine when risks exceed tolerance levels and when additional mitigation or escalation may be necessary. Effective use of risk metrics promotes early warning, informed decision-making, and continuous visibility into CalHFA's risk profile.

Risk Categories

CalHFA acknowledges five classifications of enterprise risk: compliance, financial, operational, reputational, and strategic. These categories provide a structured way to understand the types of risks that may affect the agency's ability to achieve its objectives. Using this classification, the ERM team and risk champions identify and organize

enterprise level risks within the appropriate category to support consistent analysis and discussion across the organization.

Enterprise Risk Categories	
Risk Category	**Definition**
Compliance (Regulatory & Legal)	Potential for legal, financial, or reputational harm resulting from failure to act in accordance with laws, regulations, industry standards, or internal policies.
Financial	The possibility of losing money, assets, or failing to meet financial obligations.
Operational	Potential for loss caused by failed internal processes, people, systems, or external events.
Reputational	The potential for negative publicity, public perception or uncontrollable events to damage an organization's brand, trust, and financial health.
Strategic	Risks that affect CalHFA's ability to achieve long-term mission, goals, and strategic objectives, or to adapt to changes in the internal or external environment.

Figure 7. CalHFA's Risk Categories

The categorization of these risks forms CalHFA's risk taxonomy, which establishes a common and consistent language for discussing, documenting, and assessing risks throughout the agency. A shared taxonomy strengthens clarity across divisions and ensures that risk related information is communicated and interpreted in a uniform manner.

Because CalHFA's operating environment continues to evolve, the taxonomy is designed to be flexible. As new risks emerge, organizational priorities shift, or understanding of risk improves, the taxonomy may be updated to reflect these changes and maintain alignment with agency needs and practices.

CALIFORNIA HOUSING FINANCE AGENCY
AUDIT AND RISK MANAGEMENT COMMITTEE CHARTER
October 2024

Purpose, Role, and Functions

The Audit and Risk Management Committee (the "Committee") assists the Board of Directors in its oversight of financial reporting, accounting integrity, and enterprise-wide risk management. In performing its duties, the Committee aims to maintain effective working relationships with the Board of Directors, Agency executive management, staff, and independent auditors.

Membership

The Committee shall consist of a minimum of three voting members, selected by the Chairman of the Board. Members will serve on a rotational basis with staggered terms. The Chairman will appoint one member as the Chair of the Committee. All members should possess the appropriate qualifications, knowledge, skills, and experience to effectively carry out the Committee's responsibilities. The Committee will oversee its own succession planning for Board approval.

Authority

The Committee operates under limited powers delegated by Board Resolution 06-08 and serves in an advisory capacity concerning audits and enterprise risk matters. Management, staff, and independent auditors will provide resources to enhance the Committee's understanding of the Agency's financial reporting obligations, and any significant issues related to financial reporting, accounting, and risk management policies. All Agency employees are expected to cooperate with the Committee as requested. The Committee has the authority to conduct any review necessary to fulfill its responsibilities, including direct access to independent auditors and any other personnel within the organization. The Committee will review its duties and charter annually and make recommendations to the Board if it determines that any changes are appropriate.

Meetings

The Committee shall meet at least twice a year, with additional meetings as requested by the Chair or other members. It will report to the full Board at least once a year regarding audit processes and outcomes. All meetings of the Committee will be open to the public, following the same notice and agenda procedures as for meetings of the full Board of Directors.

Minutes

Minutes of each meeting will be prepared and distributed to all Board members. These minutes need not be verbatim and are considered public records subject to the privileges and exemptions of the California Public Records Act or other applicable law.

Duties and Responsibilities

The Committee will conduct its oversight activities in relation to the following:

Audit

1. Review with staff and applicable independent auditors the scope and extent of each such auditor's examination, including direct inquiries regarding significant risks or exposures identified and management's strategies to mitigate those risks. The review shall encompass:

    a. External reporting requirements
    b. Materiality of the Agency's activities
    c. Internal control structure
    d. Other areas covered during the audit engagement

2. Upon completion of the audit, review and discuss with Agency's management, staff, and independent auditors:

    a. Agency annual financial statements and the independent auditors' opinion(s)

b. Current accounting and reporting issues, and relevant regulatory or professional pronouncements, ensuring management keeps the Committee informed of significant developments

c. Significant changes from prior years

d. Any illegal, improper, or sensitive transactions, reporting findings to the Board

e. Significant adjustments proposed by the independent auditors

3. Review all management letter items from independent auditors and written responses from management on each comment or finding.

4. Discuss with independent auditors the level of professional competence of the Agency's financial and accounting personnel, and any relevant recommendations which the auditors may have.

5. Review and evaluate the Agency's selection process for obtaining multi-year auditing services contract with independent auditors.

6. Review legal and regulatory matters that may materially impact financial statements, compliance policies and programs.

7. Review and assess the Agency's Conflict of Interest / Code of Ethics policy and its enforcement.

Risk Management

1. Review and recommend to the Board, changes to the Agency's enterprise-wide risk management governance and framework, in line with the Agency's Strategic Plan and annual business plan objectives, including, but not limited to the following:

a. Credit risk

b. Market risk

c. Compliance risk

d. Technology and Strategic risk
e. Legal risk
f. Business Continuity

2. Review with Agency's management and staff, to identify significant enterprise risk exposures, monitor and manage existing risks, evaluate risk mitigation strategies, based on the Agency's risk tolerances, as necessary, and report findings to the Board.

3. Review with Agency's management and staff, risks related to statutory and regulatory requirements, that could potentially impact operations of the Agency and provide findings to the Board.

4. Review findings from non-financial audits and examinations conducted by government agencies, external auditors, or consultants engaged for specific purposes.

5. Review biennial State Leadership Accountability Act (SLAA) report on the effectiveness of the Agency's internal control system to reduce waste, strengthen internal controls to minimize fraud, errors, and abuse of government funds.

6. Review the annual report on information security risk assessment, focusing on key risks, and evaluate the effectiveness of practices designed to manage cybersecurity activities to reduce vulnerabilities and combat threats.