



CCPA Cybersecurity Audit Choosing the Right Path to Defensible Assurance

A practical guide for boards, executives,
privacy leaders, and assurance stakeholders



Why act now?

Organizations meeting the largest applicability threshold may have their first audit period begin as early as calendar year (CY) 2027. Because the audit evaluates both the design and operating effectiveness of cybersecurity controls throughout a full 12 month audit period, organizations should begin assessing applicability, performing readiness assessment, and addressing identified gaps now to support full-period evidence collection and testing.

KPMG LLP



What Is the CCPA Cybersecurity Audit Requirement?

California's cybersecurity audit regulations became effective on January 1, 2026. Qualifying organizations are required to complete an annual, independent cybersecurity audit when their processing of consumers' personal information presents a significant risk to consumers' security. Organizations generally become subject to the requirement if they meet any of the applicable revenue or data-processing thresholds discussed below. The required filing is a certification of completion submitted to the California Privacy Protection Agency (CPPA).

The audit should:



Assess the design and operating effectiveness of the organization's cybersecurity program across the 18 cybersecurity components prescribed by §7123.



Be conducted by a qualified, objective, and independent auditor. The auditor may be internal or external, but independence and objectivity must be demonstrable.



Be supported by specific evidence such as documentation reviewed, sampling and testing performed, and interviews conducted; audit findings should not rely primarily on management assertions.

First certification timeline

Annual gross revenue	First audit period	Certification due
Over \$100M	Jan. 1, 2027–Jan. 1, 2028	April 1, 2028
\$50M–\$100M	Jan. 1, 2028–Jan. 1, 2029	April 1, 2029
Under \$50M	Jan. 1, 2029–Jan. 1, 2030	April 1, 2030

Source: California Privacy Protection Agency, California Consumer Privacy Act Regulations (January 1, 2026).



Who is Subject to the Audit?

A business is required to complete a cybersecurity audit if its processing of consumers' personal information presents a significant risk to consumers' security. Under the CCPA regulations, a business is considered to present such risk if any of the following conditions apply:



50% or more of annual revenue from selling or sharing personal information; or

50%



Annual gross revenue over \$26.625 million and processing personal information of 250,000+ consumers or households; or

> \$26M



Annual gross revenue over \$26.625 million and processing sensitive personal information of 50,000+ consumers.

> \$26M

The annual gross revenue threshold increased from \$25 million to \$26.625 million effective January 1, 2025 and is adjusted in odd-numbered years to reflect changes in the Consumer Price Index (CPI).

Source: California Privacy Protection Agency, California Consumer Privacy Act Regulations (January 1, 2026); California Privacy Protection Agency, Updated Monetary Thresholds in CCPA (December 17, 2024; effective January 1, 2025).





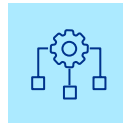
Choosing an Audit Compliance Vehicle

Organizations generally have two primary pathways for satisfying the CCPA cybersecurity audit requirement. A key consideration when selecting an audit vehicle is whether the auditor can satisfy the regulation's independence and objectivity requirements. While the regulations permit the use of either Internal Audit or an external auditor, organizations should evaluate independence considerations before selecting an audit approach.



Option 1 – Internal Audit-Led Cybersecurity Audit

Where Internal Audit serves as the independent auditor and performs the cybersecurity audit. This approach may be appropriate for organizations with a mature Internal Audit function that can satisfy the regulation's independence and objectivity requirements.

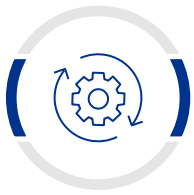


Option 2 – External Audit Path

Where an independent third-party auditor performs the cybersecurity audit through an appropriate external reporting model. This approach may be appropriate for organizations seeking external assurance, greater stakeholder confidence, specialized cybersecurity audit expertise, or the ability to leverage existing external audit and attestation activities, such as SOC examinations, or other attestation reports with overlapping scopes.

The appropriate vehicle depends on factors such as auditor independence, reporting objectives, evidence maturity, stakeholder expectations, governance structure, and overall implementation strategy.





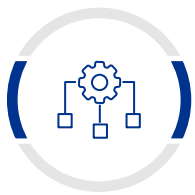
Option 1—Internal Audit-Led CCPA Cybersecurity Audit

Internal vehicle	Best fit	Benefits	Common gaps to address
Internal Audit-Led Cybersecurity Audit	- Organizations with a mature and independent Internal Audit function. - Organizations seeking to integrate the cybersecurity audit into existing audit plans and risk assessment activities. - Organizations with established cybersecurity governance and control ownership structures. - Organizations seeking to supplement Internal Audit capabilities through a co-sourced model while maintaining Internal Audit ownership of audit conclusions.	- Leverages Internal Audit knowledge of business processes, systems, data flows, and control owners. - Integrates naturally into annual audit planning and enterprise risk management activities. - Enables earlier identification of control deficiencies and remediation opportunities. - Supports continuous monitoring and repeatable annual audit execution. - Allows Internal Audit to leverage specialized cybersecurity expertise through co-sourced resources where necessary. - May represent a complete compliance path when independence and objectivity requirements are demonstrably satisfied.	- Auditor independence and objectivity may need to be formally assessed and documented. - In-house Internal Audit may lack specialized cybersecurity expertise required to evaluate all applicable cybersecurity domains. - Existing Internal Audit methodologies may require enhancement to address all applicable CCPA cybersecurity audit requirements. - Additional procedures may be needed to support full-period operating effectiveness testing and evidence requirements. - Some stakeholders may seek supplemental external validation in addition to Internal Audit conclusions.

Key Independence Considerations

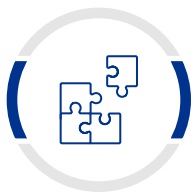
Organizations selecting the Internal Audit vehicle should evaluate whether auditor independence, objectivity, and freedom from inappropriate influence, as required by the regulations, can be demonstrated. Internal Audit should not be responsible for designing, implementing, operating, maintaining, or remediating the cybersecurity activities being audited. Organizations should also assess whether reporting relationships, oversight structures, or other governance arrangements could reasonably impair the auditor's ability to exercise objective and impartial judgment. Internal Audit may leverage co-sourced cybersecurity specialists to provide technical expertise, provided responsibility for audit conclusions remains independent from cybersecurity management and control ownership.

Source: California Privacy Protection Agency, California Consumer Privacy Act Regulations, §7122 (January 1, 2026).



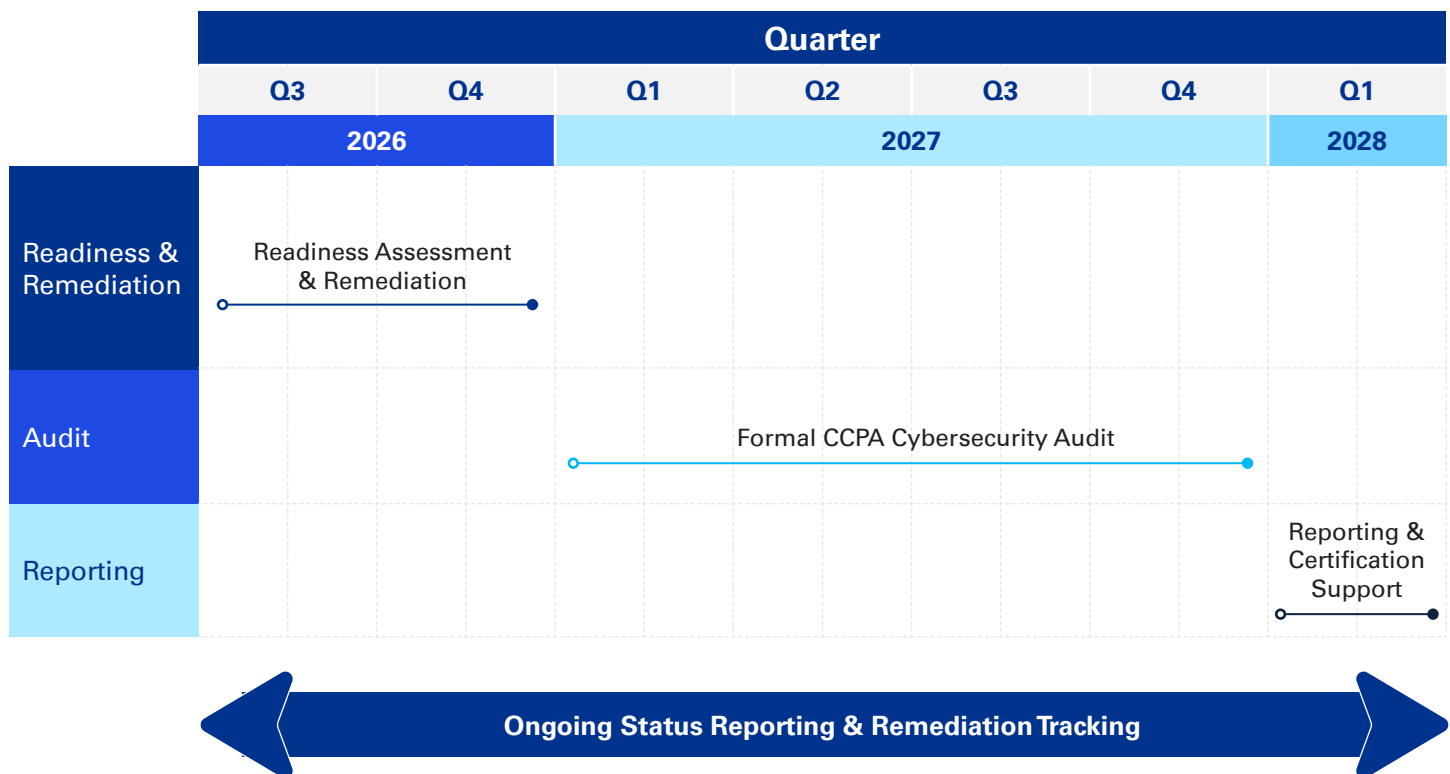
Option 2—External Audit Path

External vehicle	Best fit	Benefits	Common gaps to address
AT-C 205 examination	- Public companies - Audit committee driven requests - High-risk organizations - Organizations seeking an independent attestation report under recognized professional standards	- External assurance under recognized standards - Independent auditor opinion - May provide enhanced external credibility and rigor - Clearly aligns with “independent audit” expectations - Can directly support management certification efforts	- Mature documentation may not exist across all CCPA domains - Management assertion may need further development - Defined criteria and scope may need formalization - Additional evidence may be required to support operating effectiveness across the audit period
SOC 2+ with CCPA components	- Organizations with an existing mature SOC 2 program - Organizations seeking to leverage existing assurance activities - Organizations with existing control coverage that aligns to applicable CCPA components - Organizations with established governance, assurance and evidence collection practices	- Many SOC 2 controls and testing activities can be mapped to the CCPA cybersecurity audit components - Leverages existing SOC 2 governance, evidence collection, and reporting structure - Reduces duplicate testing where existing control coverage aligns to applicable CCPA components - Provides an efficient path for organizations with mature assurance programs	- SOC reporting period may not align with the required CCPA audit period - In-scope systems, people, and processes may not fully encompass all California personal information processing activities - Existing Trust Services Criteria may not address all applicable CCPA components - Supplemental procedures may be needed to address CCPA-specific expectations



Readiness Assessment— Separate Preparatory Phase

Readiness is not a compliance vehicle. It is a preparatory phase used to determine applicability, scope, audit vehicle selection, assess readiness, governance considerations, and provide insights that can support management in the development of full-period operating effectiveness (TOE) strategy before the formal audit period begins. Readiness activities may support either an Internal Audit or External Audit pathway but do not constitute the formal cybersecurity audit.



Source: KPMG LLP (US), *CCPA Cybersecurity Audit: Choosing the Right Path to Defensible Assurance* (2026).

Illustrative timing

Readiness assessment and remediation should occur in CY26 so the organization can enter the CY27 audit period with defined scope, remediated gaps, evidence-retention practices, and testing procedures in place.

Readiness workstream	What it should answer	Output/benefit
Applicability and scope	Is the business in scope? Which systems, applications, databases, vendors, and processing activities process California personal information?	Defensible scope perimeter and exclusion rationale.
Vehicle selection	Should the organization use Internal Audit as the audit vehicle or pursue external audit?	Decision memo comparing Internal Audit and External Audit options, independence considerations, reporting objectives, cost, timeline, and evidence maturity.
Control and criteria mapping	Which existing SOC, ISO, SOX, cyber, and internal audit controls map to each applicable §7123 component?	Reusable control inventory and gap list.
Period and TOE plan	How will the organization cover the full audit period and demonstrate operating effectiveness over time?	Testing calendar with interim, roll-forward, and year-end procedures.
SOC/ISO/internal audit leverage assessment	Do existing reports cover the right period, scope, criteria, evidence, and operating effectiveness?	Clear leverage strategy: reuse, supplement, or perform new procedures.
Independence and governance	Who audits? Who owns controls? Who remediates? Who signs the certification?	Independence memo, Internal Audit SOD structure, and executive certification support model.
Remediation roadmap	What gaps must be remediated before the formal audit period or before year-end testing?	Prioritized remediation plan with owners and target dates.



Leverage Existing Work: Identifying and Closing Gaps

An organization may use cybersecurity audits, assessments, or evaluations prepared for another purpose if the work satisfies the applicable CCPA cybersecurity audit requirements, either on its own or through supplementation. The practical question is whether the existing work provides sufficient evidence for the required audit period, scope, criteria, operating effectiveness expectations, and auditor independence requirement.

Source: California Privacy Protection Agency, California Consumer Privacy Act Regulations (January 1, 2026).

Potential gap	Why it matters	How to close it
Period gap	The first large-company CCPA audit period spans 1/1/2027 to 1/1/2028. Existing SOC or internal audit reports may have a different period.	Perform bridge and/or roll-forward procedures to cover the gap period. Depending on risk and evidence availability, this may include inquiry, roll-forward/roll-back testing, sample testing, inspection of logs, or additional TOE procedures.
Scope gap	SOC, ISO, or Internal Audit coverage may not include all systems, processes, third parties, or data flows involving California personal information.	Map personal information flows and systems to the report scope. Add systems or perform supplemental procedures where California personal information is outside the current report boundary.
Criteria gap	SOC Trust Services Criteria, ISO 27001 controls, or internal audit programs may not map one-for-one to all applicable §7123 components.	Prepare a CCPA criteria mapping and identify missing components. Add CCPA-specific controls or targeted audit procedures for missing components.
TOE evidence gap	The audit requires evidence that controls operated effectively throughout the covered period, not merely that controls existed or were assessed at a point in time.	Plan interim and year-end TOE testing. For full-period CY27 coverage, define interim testing, roll-forward procedures, deficiency remediation, and year-end completion before certification.





Choosing the Right Audit Approach

Organizations generally have two primary pathways for satisfying the CCPA cybersecurity audit requirement: an Internal Audit-led approach or an External Audit approach. Both approaches may be viable, provided the resulting audit satisfies the independence, evidence, reporting, and audit requirements established by the regulation.

When evaluating alternatives, organizations should consider:



Independence and objectivity requirements;



Availability of qualified cybersecurity audit resources;



Stakeholder expectations;



Existing assurance activities that may be leveraged; and



The effort required to produce a defensible cybersecurity audit and support the required certification of completion.

Organizations seeking greater external credibility, independent validation, or specialized cybersecurity audit expertise may find an External Audit approach advantageous, while organizations with a mature and independent Internal Audit function may find an Internal Audit-led approach sufficient.

Regardless of the vehicle selected, the audit should be supported by sufficient evidence, address the applicable audit criteria, evaluate the relevant cybersecurity program components, document identified gaps and remediation activities, and support management's certification of completion.



Authors



Doron Rotman
National Cyber and Privacy Co-Leader
Managing Director,
Technology Assurance—Audit
KPMG LLP
T: 650-575-4228
E: drotman@kpmg.com



Charles Murray
Managing Director,
Cyber & Tech Risk—Advisory
KPMG LLP
T: 313-230-3074
E: cmurray@kpmg.com



Ying Liu
Director,
Technology Assurance—Audit
KPMG LLP
T: 630-281-9855
E: yingliu3@kpmg.com



Ruixiang Wu
Director,
Technology Assurance—Audit
KPMG LLP
T: 212-954-4006
E: ruixiangwu@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



[kpmg.com](https://www.kpmg.com)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS043759-1A