BDO



California CCPA Cybersecurity Audit Requirement

A substantial number of companies are now required to complete an annual cybersecurity audit with executive management certifying to Cal Privacy that such audit has been completed. The required audit period of coverage begins as early as January 1, 2027, for many businesses.

The California Privacy Protection Agency (Cal Privacy) is responsible for implementing and enforcing the California Consumer Privacy Act of 2018 (CCPA) that established broad privacy protections for California consumers. Cal Privacy published the final CCPA regulations in September 2025, which are now effective.

Importantly, the CCPA regulations define the requirements for the annual cybersecurity audit (CCPA Cybersecurity Audit) that businesses are required to complete when their processing of consumers' personal information presents significant risk to consumers' security as set forth in section 7120, subsection (b).



IMPORTANCE OF CCPA COMPLIANCE

California's privacy standards continue to raise the bar, and the latest CCPA requirements warrant attention for any company handling California consumer data. In practical terms, the latest CCPA rules center on three key obligations: 1) cybersecurity audits, 2) risk assessments, and 3) specific governance over the use of automated decision-making technologies (ADMT). This is important because regulators increasingly expect organizations not only to protect personal information, but also to demonstrate, document, and defend how they collect, use, and process it.

The stakes for noncompliance are significant. Enforcement and litigation exposure can be severe, with current penalties up to $2,663 per nonintentional violation (i.e., per affected consumer) and up to $7,988 per intentional violation or those involving minors' personal information. To put that in perspective, if 500,000 California consumers were impacted, potential exposure could reach $1.3 to $4 billion.

CYBERSECURITY AUDIT APPLICABILITY (WHO DOES THE AUDIT APPLY TO?)

The cybersecurity audit applies to a subset of for-profit entities that process California consumers' personal information and meet any of the following:

- Derive 50% or more of their annual revenue from selling or sharing consumers' personal information; or
- As of January 1, of the preceding year, has annual gross revenue of $26.625 million; and
- Processes personal information of 250,000 or more California consumers or households in the preceding calendar year; or
- Processes sensitive personal information of 50,000 or more California consumers in the preceding calendar year.

It should be noted that employee data and corresponding systems housing employee data are considered within the scope of consumer data under CCPA.

REQUIRED AUDIT PHASE-IN PERIODS AND DUE DATES (WHEN IS THE FIRST AUDIT DUE?)

The due date for a business's first cybersecurity audit is phased in over three years, depending on the annual gross revenue as shown below.

Year	Annual Gross Revenue	Required Audit Period	Required Audit Report Completion
2026	More than $100M	1/1/2027 – 1/1/2028	4/1/2028
2027	Between $50M - $100M	1/1/2028 – 1/1/2029	4/1/2029
2028	Less than $50M	1/1/2029 – 1/1/2030	4/1/2030

SCOPE

The CCPA Cybersecurity Audit and Audit Report are required to cover:

- How the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.
- The business's establishment, implementation, and maintenance of its cybersecurity program and how the business implements and enforces compliance with its cybersecurity program.
- The following eighteen components of the cybersecurity program:
  - Authentication
  - Encryption of Personal Information
  - Account Management and Access controls
  - Inventory and Data/System Mapping
  - Secure Configuration
  - Vulnerability Scanning and Penetration Testing
  - Audit Log Management
  - Network Monitoring and Defenses
  - Antivirus/Anti-malware
  - System Segmentation
  - Port and Protocol Management
  - Cybersecurity Awareness
  - Training and Education
  - Secure Development Practices
  - Third-Party Oversight
  - Data Retention and Disposal
  - Incident Response
  - Business Continuity and Disaster Recovery

EXECUTIVE MANAGEMENT CERTIFICATION

The CCPA regulations require that a business's executive management annually certify to Cal Privacy via its website that they have completed their annual cybersecurity audit. They are not required to submit their audit reports, but they must be available to Cal Privacy upon request. The written certification, however, must be completed and submitted to the Agency via its website at cppa.ca.gov.



CYBERSECURITY AUDIT APPROACHES

A client has options in determining what form of audit report may be most appropriate and efficient based on their existing portfolio of security audit reports and certifications.

While the regulation is specific about the security requirements that must be addressed, it is not prescriptive about the type of audit report produced. It references the NIST cybersecurity framework as one option while also referencing AICPA, ISACA, ISO and PCAOB auditing procedures and standards. While the regulation refers to the "audits", the guidance allows for the use of frameworks that are governed by organizations that are oriented towards "assessments" such as NIST CSF and ISO.

Our point of view is that different reporting approaches may be better suited for different companies. We work with our clients to determine an approach that aligns with their needs and circumstances.

- In some cases, a SOC 2 Type 2 plus report covering the cybersecurity requirements as additional criteria may be an effective approach.
- In cases where the company does not have an existing business requirement for SOC reports for this standard, a custom report based on NIST CSF, ISO 27001 or SOC for Cybersecurity may be appropriate.
- In other cases, companies may choose to complete the process internally through an independent assessment (through internal audit, as one example) and comply with the independence requirements of the standard.

The regulation notes that the auditor may be internal or external to the business, and the audits are to be conducted by a qualified, objective, and independent auditor who is free from management influence and capable of exercising impartial judgment. To preserve independence, the auditor may not design, implement, operate, or otherwise participate in activities that are subject to audit, and internal auditors, if leveraged for the audit, must maintain organizational reporting lines separate from the cybersecurity function. Additional details from the regulation are noted in *§ 7122. Thoroughness and Independence of Cybersecurity Audits*.



OTHER UPDATED REQUIREMENTS TO CONSIDER

Under the California privacy regulations, in addition to the cybersecurity audit requirement, for-profit entities need to take into consideration:

- Performing risk assessments for high-risk processing activities beginning **January 1, 2026**. Risk assessments for qualifying activities in existence before 2026 must be completed by **December 31, 2027**, and the first annual risk assessment summaries must be submitted to the Cal Privacy by **April 1, 2028**.
- Providing individuals with a pre-use notice describing the use of **Automated Decision-Making Technology (ADMT)**. Consumers must be informed when ADMT is used, and, where required, must be given the opportunity to **opt out** of its use in connection with significant decisions.





CONTACT US



BINITA PRADHAN
West - Third Party Assurance Market & Practice Leader
bpradhan@bdo.com



MARK LUNDIN
Third Party Assurance Principal
mlundin@bdo.com



GREG SCHU
Cybersecurity & Compliance Principal
gschu@bdo.com



ANDREW BELSICK
Managing Director, Cyber Practice
abelsick@bdo.com

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.